UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА «РИ-2016»

ЮБИЛЕЙНАЯ XV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2016 года

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2016

http://spoisu.ru

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА «РИ-2016»

ЮБИЛЕЙНАЯ XV САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 26-28 октября 2016 года

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2016

http://spoisu.ru

УДК (002:681):338.98

Р32

Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская
Р32 международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. \ СПОИСУ. – СПб, 2016. – 599 с.
ISBN 978-5-906841-68-1.

Сборник охватывает широкий круг направлений: Региональная политика информатизации. Электронное правительство; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые проблемы информатизации; Информационно-аналитическое обеспечение органов государственной власти; Информационно-психологическая безопасность; Информационные технологии в экономике; Информационное обеспечение финансово-кредитной сферы и бизнеса; Информационные технологии в критических инфраструктурах; Информационные технологии в производстве; Информационные технологии на транспорте; Информационные технологии в научных исследованиях; Информационные технологии в образовании; Информационные технологии в медицине и здравоохранении; Информационные технологии в экологии; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационные технологии в метеорологии Арктического региона; Информационные технологии в издательской деятельности, полиграфии и дизайне; Геоинформационные системы; Информационные технологии управления риском в социально-экономических системах; Информационные технологии в социокомпьютинге; Распределенные информационно-вычислительные системы, грид-технологии, а также материалы молодежных научных школ «Региональная информатика и проблемы устойчивого развития» и «Безопасные информационные технологии». Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области информатизации, связи и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.П. Заболотский, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 12.10.2016. Формат 60x84⅛. Бумага офсетная.
Печать – трафаретная. Усл. печ. л. 37.4. Тираж 500 экз. Заказ № 1201
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-906841-68-1

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2016 г.
© Авторы, 2016 г.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

REGIONAL INFORMATICS «RI-2016»

XV ANNIVERSARY ST. PETERSBURG INTERNATONAL CONFERENCE

St. Petersburg, October 26-28 2016

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2016

http://spoisu.ru

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство связи и массовых коммуникаций Российской Федерации
- Министерство образования и науки Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий Российской академии наук
- Санкт-Петербургский научный Центр Российской академии наук
- Санкт-Петербургский институт информатики и автоматизации Российской академии наук
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- Российский фонд фундаментальных исследований
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- ФГУП «ЦентрИнформ»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Петербургский государственный университет путей сообщения Императора Александра I
- Санкт-Петербургский политехнический университет Петра Великого
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет промышленных технологий и дизайна
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
- Санкт-Петербургский университет МВД России
- Санкт-Петербургский институт экономики и бизнеса
- Смольный институт Российской академии образования
- Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
- Группа компаний «Омега»
- АО «Концерн «НПО «Аврора»
- АО «Научно-исследовательский институт программных средств»
- АО «Научно-производственное объединение «Импульс»
- АО «Институт инфотелекоммуникаций»
- ОАО «Центр компьютерных разработок»
- ЗАО «Институт телекоммуникаций»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ООО «АСБ»
- ООО «Геонавигатор»
- ООО «ИнТехСервис»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии информатизации образования

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

Полтавченко Георгий Сергеевич	Губернатор Санкт-Петербурга
Макаров Вячеслав Серафимович	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Алферов Жорес Иванович	Вице-президент Российской академии наук, председатель Президиума Санкт-Петербургского научного Центра Российской академии наук, Лауреат Нобелевской премии
Велихов Евгений Павлович	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук
Васильева Ольга Юрьевна	Министр образования и науки Российской Федерации
Никифоров Николай Анатольевич	Министр информационных технологий и связи Российской Федерации

ПРЕЗИДИУМ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Председатель Программного комитета, сопредседатель Научного совета по информатизации Санкт-Петербурга
Юсупов Рафаэль Мидхатович	Председатель Организационного комитета, директор Санкт-Петербургского института информатики и автоматизации Российской академии наук
Говорунов Александр Николаевич	Вице-губернатор Санкт-Петербурга - руководитель Администрации Губернатора Санкт-Петербурга
Кучерявый Михаил Михайлович	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Чамара Денис Петрович	И.о. председателя Комитета по информатизации и связи Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Васильев Владимир Николаевич	Председатель совета ректоров Санкт-Петербурга, ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук

Заместитель председателя Организационного Комитета

Чамара Денис Петрович	И.о. председателя Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Алейник Ярослав Александрович	Руководитель Группы компаний «Омега»
Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Басков Вячеслав Дмитриевич	Генеральный директор ООО «НеоБИТ»
Бакурадзе Дмитрий Викторович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Блажис Анатолий Константинович	Директор ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Бобрович Владимир Юрьевич	Заместитель генерального директора по развитию ОАО «Концерн «НПО «Аврора»
Богданов Владимир Николаевич	Директор ФГУП «ЦентрИнформ»
Борисов Николай Валентинович	Директор Междисциплинарного центра Санкт-Петербургского государственного университета
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Гаценко Олег Юрьевич	Генеральный директор АО «Научно-исследовательский институт программных средств»
Герус Евгений Валерьевич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»
Гоголь Александр Александрович	Советник ректора, заведующий кафедрой Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Григорьев Владимир Александрович	Генеральный директор ООО «Лаборатория инфокоммуникационных сетей»
Гуца Анатолий Григорьевич	Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна
Жданов Сергей Николаевич	Заместитель генерального директора АО ВТБ Девелопмент
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций»
Заболотский Вадим Петрович	Главный научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой Санкт-Петербургского политехнического университета Петра Великого
Зубков Юрий Сергеевич	Действительный государственный советник Санкт-Петербурга 3 класса
Игнатьев Михаил Борисович	Заслуженный профессор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Игумнов Владимир Вячеславович	Главный конструктор АО «Научно-производственное объединение «Импульс»
Идрисов Рустам Фидайович	Директор Центра исследований проблем безопасности Российской академии наук
Ипатов Олег Сергеевич	И.о. проректора Санкт-Петербургского политехнического университета Петра Великого
Искандеров Юрий Марсович	Генеральный директор ООО «Инновационный центр транспортных исследований»

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Кефели Игорь Федорович	Заведующий кафедрой Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова
Корниенко Анатолий Адамович	Заведующий кафедрой Петербургского государственного университета путей сообщения Императора Александра I
Кузичкин Александр Васильевич	Заместитель директора АО «НИИ телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кутузов Владимир Михайлович	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Лезунова Наталья Борисовна	Директор Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского Научного центра Российской академии наук
Михайлов Николай Семенович	Технический директор Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Молдовян Александр Андреевич	Заместитель директора по информационной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Николаев Алексей Юрьевич	Генеральный директор ЗАО «Эврика»
Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Ныркov Анатолий Павлович	Заведующий кафедрой Государственного университета морского и речного флота имени адмирала С.О. Макарова
Оводенко Анатолий Аркадьевич	Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения
Остапенко Александр Николаевич	Генеральный директор ЗАО «Лаборатория противодействия промышленному шпионажу»
Панычев Александр Юрьевич	Ректор Петербургского государственного университета путей сообщения Императора Александра I
Перепелица Сергей Николаевич	Генеральный директор ООО «ИнТехСервис»
Пильдес Майя Борисовна	Директор Академической Гимназии № 56 Санкт-Петербурга, Народный учитель Российской Федерации
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пролетарский Андрей Викторович	Декан Московского государственного технического университета им. Н.Э. Баумана
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»
Рунеев Анатолий Юрьевич	Генеральный директор ФГУП «Научно-исследовательский институт «Рубин»
Силла Евгений Петрович	Ученый секретарь Санкт-Петербургского института информатики и автоматизации Российской академии наук
Симонов Михаил Владимирович	Главный консультант директора ФГУП «ЦентрИнформ»
Солодянников Александр Владимирович	Генеральный директор ООО «АСБ»

Соложенцев Евгений Дмитриевич	Заведующий лабораторией Института проблем машиноведения Российской академии наук
Степанов Александр Георгиевич	Профессор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Строганов Дмитрий Викторович	Проректор Московского автомобильно-дорожного государственного технического университета (МАДИ)
Тимофеев Александр Васильевич	Председатель Правления Санкт-Петербургского союза дизайнеров
Тихомиров Сергей Григорьевич	Генеральный директор ОАО «Центр компьютерных разработок»
Ткач Анатолий Федорович	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук
Устинов Игорь Анатольевич	Генеральный директор АО «Научно-производственное объединение «Импульс»
Федоров Андрей Евгеньевич	Директор института – заместитель генерального директора АО «Концерн «НПО «Аврора»
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук
Чугунов Андрей Владимирович	Заведующий кафедрой, директор Центра технологий электронного правительства Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Шерстюк Юрий Михайлович	Генеральный директор АО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор АО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций»
Ипатов Олег Сергеевич	И.о. проректора Санкт-Петербургского политехнического университета Петра Великого

Члены Программного Комитета – руководители и секретари секций

Координатор Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

Ученый секретарь Конференции

Заболотский Вадим Петрович	Главный научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

Главный информационный спонсор Конференции

«Компьютер Информ»	Газета о передовых инфокоммуникационных технологиях, продуктах, решениях для руководителей предприятий и организаций, отделов АСУ, ведущих специалистов и служб ИКТ, www.ci.ru

СОСТАВ ПРОГРАММНОГО КОМИТЕТА КОНФЕРЕНЦИИ

Азаров Артур Александрович	Научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Александров Виктор Васильевич	Заведующий лабораторией автоматизации научных исследований Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф., лауреат премии Правительства РФ в области науки и техники
Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор кафедры Санкт-Петербургского государственного морского технического университета, д-р техн. наук, проф.
Алексеев Вадим Владимирович	Сотрудник городского центра экспертиз, канд. техн. наук
Барабаш Павел Александрович	Декан факультета информационных технологий, ученый секретарь Ученого совета Смольного института Российской академии образования, канд. техн. наук, доц.
Баранова Евгения Васильевна	Профессор кафедры методики информационного и технологического образования института компьютерных наук и технологического образования Российского государственного педагогического университета им. А.И. Герцена, д-р пед. наук, проф.
Бариков Леонид Николаевич	Доцент Санкт-Петербургского государственного университета аэрокосмического приборостроения, канд. техн. наук, доц.
Берекет Виктор Максимович	Генерал-майор полиции, заместитель начальника Санкт-Петербургского университета МВД России по научной работе, канд. юрид. наук, доц.
Бессонова Екатерина Евгеньевна	Ассистент кафедры безопасных информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, канд. техн. наук
Бирюков Михаил Александрович	Адъюнкт Военной академии связи им. С.М. Буденного
Блюдов Антон Александрович	Доцент кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I, канд. техн. наук
Богданов Виталий Олегович	Программист Санкт-Петербургского института информатики и автоматизации Российской академии наук
Бузников Анатолий Алексеевич	Заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), заслуженный деятель науки РФ, д-р техн. наук, проф.
Вассоевич Андрей Леонидович	Профессор кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, д-р филос. наук, проф.
Воробьев Владимир Иванович	Главный научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, дважды лауреат премии Правительства России в области образования
Гончаров Вадим Владимирович	Менеджер ООО «Монтаж Электросистем», канд. экон. наук
Горенбургов Михаил Абрамович	Профессор Санкт-Петербургского экономического университета, д-р экон. наук, проф.

Горохов Владимир Леонидович	Профессор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, д-р техн. наук, проф.
Грозный Алексей Зорьевич	Заместитель директора Санкт-Петербургского информационно-аналитического центра
Денисова Дарья Михайловна	Научный сотрудник лаборатории биомедицинской информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Домбровская Лариса Александровна	Профессор кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. пед. наук, доц.
Дюк Вячеслав Анатольевич	Ведущий научный сотрудник лаборатории биомедицинской информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Ефанов Дмитрий Викторович	Доцент кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I, канд. техн. наук
Ефимов Вячеслав Викторович	Директор Ленинградского отделения Центрального научно-исследовательского института связи, канд. тех. наук
Жаркова Ольга Романовна	Методист кафедры Информационных и управляющих систем Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна
Жвалевский Олег Валерьевич	Научный сотрудник лаборатории биомедицинской информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», д-р техн. наук, доц.
Зайцева Александра Алексеевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Захаров Юрий Никитич	Первый заместитель директора Санкт-Петербургского информационно-аналитического центра, канд. техн. наук, проф.
Зикратов Игорь Алексеевич	Заведующий кафедрой безопасных информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, д-р техн. наук, проф.
Ивакин Ян Альбертович	И.о. заведующего лабораторией объектно-ориентированных геоинформационных систем, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Игнатьев Михаил Борисович	Профессор Санкт-Петербургского государственного университета аэрокосмического приборостроения, д-р техн. наук, проф., действительный член Российской академии естественных наук, Senior member of the Society for Modeling and Simulation International, Distinguished Scientist of the Association of Computing Machinery
Игумнов Владимир Вячеславович	Первый заместитель генерального директора, главный конструктор АО «Научно-производственное объединение «Импульс», канд. техн. наук
Ильин Виктор Павлович	Доцент кафедры автоматизированных систем обработки информации и управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.

Казаков Александр Яковлевич	Заведующий кафедрой Высшей математики и информатики Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, д-р физ.-мат. наук, проф.
Карасев Василий Владимирович	Старший научный сотрудник лаборатории интегрированных систем автоматизированного проектирования Института проблем машиноведения Российской академии наук, канд. техн. наук
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доц., лауреат премии Правительства РФ в области образования
Кефели Игорь Федорович	Заведующий кафедрой глобалистики и геополитики Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова, заслуженный работник высшей школы РФ, д-р филос. наук, проф.
Кий Андрей Вячеславович	Доцент кафедры Военной академии связи им. С.М. Буденного, канд. техн. наук
Коваленко Александр Николаевич	Заведующий кафедрой Информационных и управляющих систем Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, канд. физ.-мат. наук, доц.
Коноплёв Георгий Асадович	Доцент Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Копыльцов Александр Васильевич	Профессор кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), профессор кафедры информационных систем Смольного института Российской академии образования, д-р техн. наук, проф.
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доц.
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Лаптев Владимир Валентинович	Проректор по научной работе Российского государственного педагогического университета им. А.И. Герцена, Вице-президент Российской академии образования, академик Российской академии образования, заслуженный деятель науки РФ, д-р пед. наук, проф.
Лебедев Илья Сергеевич	Доцент кафедры безопасных информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, д-р техн. наук, доц.
Лупал Марина Иосифовна	Специалист по учебно-методической работе факультета информационных технологий Смольного института Российской академии образования
Лысенко Владимир Александрович	Заместитель председателя учебно-методической комиссии «Информационные технологии в дизайне», руководитель Центра электронных ресурсов и технологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, д-р техн. наук, доц.
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, канд. экон. наук

Митько Арсений Валерьевич	Доцент кафедры Санкт-Петербургский государственный университет аэрокосмического приборостроения, председатель Совета молодых учёных Севера Арктической общественной академии наук, канд. тех. наук, доц.
Митько Валерий Брониславович	Председатель Санкт-Петербургского отделения секции геополитики и безопасности Российской академии естественных наук, президент Арктической общественной академии наук, доктор тех. наук, проф.
Молдовян Александр Андреевич	Заместитель директора по информационной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Никитин Александр Борисович	Заведующий кафедрой «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I, д-р техн. наук, проф.
Ныркoв Анатолий Павлович	Заведующий кафедрой Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, проф.
Паращук Игорь Борисович	Профессор кафедры Военной академии связи им. С.М. Буденного, д-р техн. наук, проф.
Пащенко Антон Евгеньевич	Научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Петров Михаил Петрович	Ведущий программист Санкт-Петербургского института информатики и автоматизации Российской академии наук
Плебанек Ольга Васильевна	Доцент кафедры глобалистики и геополитики Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова, канд. филос. наук, доц.
Поленин Владимир Иванович	Профессор Военного учебно-научного центра Военно-морского флота «Военно-морская академия им. Н.Г. Кузнецова» (ВУНЦ ВМФ), д-р техн. наук, проф.
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, д-р техн. наук, проф.
Путилин Алексей Николаевич	Заместитель главного конструктора АО «Научно-производственное объединение «Импульс», д-р техн. наук, проф.
Разживин Никита Сергеевич	Магистрант кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Романова Марина Владимировна	Ведущий программист Санкт-Петербургского института информатики и автоматизации Российской академии наук
Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Свешникова Наталья Олеговна	Доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, канд. психол. наук, доц.
Симонова Ирина Викторовна	Профессор кафедры методики информационного и технологического образования института компьютерных наук и технологического образования Российского государственного педагогического университета им. А.И. Герцена, д-р пед. наук, проф.

Смирнова Оксана Вячеславовна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), академик Российской академии образования, заслуженный деятель науки РФ, д-р техн. наук, проф., лауреат премии Правительства РФ в области образования
Согонов Сергей Александрович	Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук, доц.
Соколов Борис Владимирович	Заместитель директора по научной работе Санкт-Петербургского института информатики и автоматизации Российской академии наук, заслуженный деятель науки РФ, д-р техн. наук, проф.
Соколов Сергей Сергеевич	Начальник Управления информатизации Государственного университета морского и речного флота имени адмирала С.О. Макарова, канд. техн. наук, доц.
Соложенцев Евгений Дмитриевич	Заведующий лабораторией интегрированных систем автоматизированного проектирования Института проблем машиноведения Российской академии наук, д-р техн. наук, проф.
Татарникова Татьяна Михайловна	Профессор кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, д-р техн. наук, доц.
Тишков Артем Валерьевич	Заведующий кафедрой физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. акад. И. П. Павлова, канд. физ.-мат. наук, доц.
Токарев Владимир Семенович	Главный специалист, секретарь Научно-технического совета Санкт-Петербургского информационно-аналитического центра, канд. техн. наук, доц.
Трофимов Валерий Владимирович	Заведующий кафедрой информатики Санкт-Петербургского государственного экономического университета, д-р техн. наук, проф.
Тулупьев Александр Львович	Заведующий лабораторией теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р физ.-мат. наук, доц.
Тумалева Елена Андреевна	Доцент кафедры методики информационного и технологического образования института компьютерных наук и технологического образования Российского государственного педагогического университета им. А.И. Герцена, канд. пед. наук, доц.
Тюрин Иван Сергеевич	Магистрант кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Генеральный директор АО «Научно-производственное объединение «Импульс», канд. техн. наук
Ушакова Наталья Петровна	Заведующая лабораторией ОАО «Концерн «Научно-производственное объединение «Аврора», канд. техн. наук, доц.
Фаткиева Роза Равильевна	Старший научный сотрудник лаборатории информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доц.
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук

Ходаковский Валентин Аветикович	Заведующий кафедрой «Математика и моделирование» Петербургского государственного университета путей сообщения Императора Александра I, д-р техн. наук, проф.
Цехановский Владислав Владимирович	Заведующий кафедрой автоматизированных систем обработки информации и управления, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Шишкин Владимир Михайлович	Старший научный сотрудник лаборатории информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доц.
Шкирятов Олег Тимофеевич	Первый заместитель генерального директора по научной работе АО «Научно-производственное объединение «Импульс», д-р воен. наук, проф.
Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук, член-корреспондент Российской академии наук, заслуженный деятель науки и техники РФ, д-р техн. наук, проф., лауреат премии Правительства РФ в области образования
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. психол. наук

ПЛЕНАРНЫЕ ДОКЛАДЫ

Советов Б.Я.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ТЕНДЕНЦИИ РАЗВИТИЯ ВЫСШЕГО ОБРАЗОВАНИЯ И ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В истории Российского образования можно выделить ряд этапов, связанных с внешними и внутренними социально-экономическими условиями развития страны, но всегда состояние образования определялось государственной политикой. Корни современного образования уходят в русское просвещение, основами которого были самодержавие, православие и народность. Составляющими идеологии советского образования были патриотизм, духовность, фундаментальность, профессиональная ориентированность, доступность, непрерывность в течение всей жизни. Этому соответствовала квазиадминистративная модель образования, отвечающая отечественному опыту образования.

С 90-х годов началось усиленное копирование западной многоуровневой системы образования, что оправдывалось необходимостью вхождения Российского образования в мировую образовательную систему. В системе высшего образования стали преобладать элементы либеральной модели образования. Переход на многоуровневую систему подготовки кадров оправдывался и надеждой на сокращение срока обучения до 4 лет. Однако уровень бакалавра оказался для работодателей явно недостаточным, и пришлось пойти на реализацию второго бесплатного высшего образования – магистратуру, т.е. вместо 5 лет обучения инженера предусмотреть 6 лет обучения магистра.

В настоящее время сложившая система высшего образования оказалась неспособной удовлетворить требования работодателей. Более половины выпускников Вузов не находят работу по выбранному им профилю подготовки. На данном этапе выходом из создавшейся ситуации явилась актуализация федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) путем приближения их к профессиональным стандартам. При этом были определены профессии и должности, на которые может претендовать выпускник бакалавриата. Удовлетворение требований работодателей возможно за счет интеграции образования, науки и промышленности. Для этого необходимо изменение государственного подхода к образованию.

В настоящее время определены приоритетные направления развития образования: создание современной образовательной среды для школьника, модернизация среднего профессионального образования, развитие высшей школы как центра по созданию инноваций, продвижение современной цифровой образовательной среды (поддержка онлайн-обучения). В этих условиях крайне необходимо в рамках закона признать, что образование не услуга, а служение, поддержать экономически высшую школу как основу настоящего и будущего интеллектуального уровня развития общества. Необходимо обеспечить условия для выполнения студентами научных исследования в рамках студенческих научных обществ. Следует поддержать всевозможные структуры сотрудничества вузов, НИИ и предприятий, считать научно-педагогические школы основой воспитания и образования кадров, расширить специалитет, вернуться к аспирантуре как к научной структуре в рамках высшей школы с необходимостью завершения работы над диссертацией в период пребывания в аспирантуре, особое внимание уделить проблеме воспитания усилению связи между учителем и учеником. В условиях завершения перехода к информационному обществу и значительных достижений в области развития информационных технологий необходимо признать электронное образование четвертой формой образования для ряда возможных направлений основной подготовки, второго высшего образования и дополнительного образования (профессиональной переподготовки и повышения квалификации). В современных внешних экономических условиях и необходимости импортозамещения усиление инженерной подготовки является необходимым условием преобразования вузов в инновационные центры, что предусматривается государственной политикой, выраженной в Указах Президента страны.

Соколов Б.В., Юсупов Р.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

НЕОКИБЕРНЕТИКА: НЕОГРАНИЧЕННЫЕ ВОЗМОЖНОСТИ И ВОЗМОЖНЫЕ ОГРАНИЧЕНИЯ

Авторами доклада предлагаются методологические и методические основы неокибернетики, под которой понимается междисциплинарная наука, ориентированная на разработку методологии постановки и решения проблем анализа и синтеза адаптивных и самоорганизующихся интеллектуальных технологий и систем управления (АдИССУ) сложными объектами произвольной природы (СОПП), обладающие свойством проактивности, избирательности и операциональной замкнутости, а также способностью моделировать среду и себя в ней (кибернетика наблюдения, включающего и самого наблюдателя). В качестве основных задач неокибернетики в докладе выделены: задачи целенаправленного и обоснованного создания (расширения разнообразия в интеллектуальных систем управления (СУ), сужения разнообразия внешней среды); задачи декомпозиции (композиции), агрегирования (дезагрегирования), координация, линеаризация, аппроксимации, релаксации при моделировании, анализе и синтезе АдИССУ СОПП; задачи управления структурной динамикой АдИССУ; задачи квалиметрии моделей и полимодельных комплексов АдИССУ; традиционные задачи «классической кибернетики I порядка» применительно к АдИССУ.

Основными подходами и принципами неокиберники являются структурно-математический и категорийно-функторный подходы, системный подход и его концепции и принципы, включающие в себя: принципы неокончательных решений, поглощения разнообразия, иерархической компенсации, дополнительности, полимодельности и многокритериальности, самоподобного рекурсивного описания и моделирования объектов исследования, гомеостатического баланса взаимодействия; преодоление принципа разделения; принципы, положенные в основу создания онтологий; принципы Ле-Шателье–Брауна; принципы декомпозиции и агрегирования; принцип рационального многокритериального компромисса при наличии неустранимых пороговых информационных и временных ограничений; принцип интерактивного итерационного формирования решения в условиях неопределенности и противоречивости исходной информации.

К числу нерешенных проблем неокибернетики можно, в первую очередь, отнести проблемы организации и проведения междисциплинарных исследований по проблемам управления развитием АдИССУ СОПП; исследование базовых свойств АдИССУ (самоконфигурирование, самообслуживание, самооптимизация, самозащита) и факторов на них влияющих; разработка методов, алгоритмов, моделей обоснования, анализа и синтеза адаптивных информационных технологий организации и реализации процессов функционирования АдИССУ с учетом объективных потребностей в соответствующих данных, информации и знаниях. К настоящему времени авторами доклада в рамках проводимых ими междисциплинарных исследований по формированию основ неокибернетики был получен ряд интересных результатов в области управления структурной динамикой сложных технических систем (СТС) в различных предметных областях. В частности, было установлено, что одной из основных особенностей современных СТС является то, что их параметры и структуры на различных этапах жизненного цикла изменяются под действием объективных и субъективных причин. В этих условиях для повышения (сохранения) уровня работоспособности и возможностей СТС, либо обеспечения наилучших условий деградации указанных систем необходимо осуществлять управление их структурами (в том числе управление реконфигурацией структур СТС).

Черешкин Д.С., Сичкарук А.В.
Россия, г. Москва, Федеральный исследовательский центр «Информатика и управление» РАН

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ОБЪЕКТОВ

Происходящий сегодня практически во всем мире процесс построения информационного общества изменяет многое в жизни как отдельного человека, так и общества и государства в целом. Наряду с положительным, широко масштабное использование информационных технологий, средств их реализации, систем телекоммуникаций, включая интернет, порождает возникновение множества проблем, среди которых приоритетной является проблема обеспечения безопасности критически важных объектов (КВО) любой национальной инфраструктуры. Сегодня, в условиях усложнения производственных процессов, процессов управления и общественных отношений существенно повышается роль и значимость безопасности широко применяемых автоматизированных человеко-машинных систем, программно-аппаратных комплексов, систем связи, поскольку нарушение их нормативной работы может привести к сложно прогнозируемым негативным воздействиям на многие территории и страны. Появление нового вида слабо прогнозируемых угроз – кибернетических, ориентированных непосредственно на нарушение функционирования именно этого класса систем также существенно изменяет эффективность ранее принятой идеологии обеспечения безопасности КВО и требует формирования нового подхода к обеспечению комплексной безопасности сложных процессов и объектов, отличного от подхода 2000-х. Это отражается и в проектах новых директивных

документах – Доктрины информационной безопасности РФ, Концепции информационно-аналитической системы мониторинга показателей состояния национальной безопасности РФ и ряде других.

Современная идеология обеспечения безопасности КВО должна строится на новых принципах – обеспечение комплексной безопасности всех критических элементов объекта за счет: мониторинга состояния их уязвимостей; управления безопасностью на основе управления рисками возможного нарушения регламентных режимов работы объекта; прогнозирования его возможных состояний на основе определения рисков; выработки вариантов разрешения потенциальной критической ситуации.

Все выше сказанное требует или создания новых типов автоматизированных систем обеспечения безопасности (АСОБ) взамен существующих сегодня или существенной их модернизации. Очевидно, что второй путь в условиях финансового кризиса в стране более предпочтителен.

Предлагается совершенствования существующих АСОБ за счет:

- интеграции существующих разрозненных подсистем АСОБ по каждому виду угроз в систему обеспечения комплексной безопасности КВО;
- создание в составе АСОБ подсистемы мониторинга состояния известных уязвимостей и критических точек процессов;
- расчетов рисков возникновения критических ситуаций за счет невыполнения нормативных требований по безопасности и/или низкой эффективности применяемых средств противодействия;
- разработки и встраивания в АСОБ системы поддержки принятия решений (СППР) на каждом уровне иерархии системы управления КВО.

Предлагается методика решения поставленных выше задач на основе СППР в АСОБ КВО.

Система поддержки принятия решений – диалоговая автоматизированная информационная система в составе АСОБ, обеспечивающая расчетно-аналитическим путем оценку потенциальной и/или существующей критической ситуации нарушения состояния безопасности элементов и объекта в целом, сравнение полученной оценки с заданным ее допустимым значением и представляющая лицу, принимающему решение (ЛПР) необходимую для этого информацию.

В состав СППР входит блок интерфейса с оператором и подсистемой сбора информации, базы данных и расчетно-аналитический блок вычисления величины рисков возникновения критической ситуации, блок формулирования и оценки альтернативных решений. СППР должна работать с любыми видами исходной информации – количественные и качественные показатели, не структурированная информация, экспертные оценки.

В зависимости от данных, с которыми работают СППР, их можно разделить на оперативные и стратегические.

Системы первого типа предназначены для оперативного управления текущей ситуации в реальном масштабе времени. В нашем случае, на основании получаемой информации любого типа, рассчитываются величины рисков возможности возникновения критической ситуации (нарушение безопасности) вследствие не выполнения нормативных требований обеспечения безопасности на конкретной уязвимости объекта.

Системы второго типа, обеспечения стратегической поддержки принятия решений, ориентированы на прогнозирование рисков возможности возникновения критической ситуации на основе анализа большого количества информации из разных источников о состоянии с привлечением сведений, содержащихся в системах, аккумулирующих опыт решения проблем. Важным компонентом этих систем является использование правил принятия решений и учета приоритетов ЛПР, которые на основе агрегированных данных подсказывают экспертам выводы и придают системе черты систем искусственного интеллекта.

Очевидно, что формируемая СППР должна обладать характерными чертами обоих рассмотренных выше типов, т.е. обеспечивать как решение задач оперативного управления, так и прогнозирования возможного возникновения критической ситуации.

Формирование СППР в составе АСОБ, при выполнении перечисленных выше требований по ее модернизации, выдвигает, в свою очередь ряд специфических, именно для СППР, требований. Эти требования определяют:

- выбор методики оценки величины рисков возможности появления на объекте критической ситуации (нарушение нормативных режимов деятельности, авария, террористический акт и т.д.) и ее программно-аппаратная реализация;
- выбор состава, вида представления, методов сбора, хранения, доступа и обработки необходимой для анализа и расчетов информации;
- организацию и регламенты взаимодействия СППР с АСОБ и руководством объекта, ответственным за обеспечение безопасности;
- вид и формы представления получаемых результатов.

Ограниченные объемы публикации позволяют подробно рассмотреть только вопрос выбора методики оценки величины рисков возможности появления на объекте критической ситуации.

Предлагается использовать методику, разработанную в ИСА РАН, хорошо зарекомендовавшую себя при решении конкретных задач обеспечения безопасности на ряде реальных объектов (ЦБ РФ, а/п Шереметьево, МЧС РФ). Очевидно, что основная задача СППР – реализация данной методики в процессе ее функционирования.

Основная идея методики – определение эффективности используемой на объекте системы обеспечения безопасности (СОБ) и входящих в ее состав средств защиты для каждой уязвимости объекта при возможном воздействии на нее комплекса любого типа угроз, а также выполнение нормативных требований по обеспечению безопасности с последующей агрегации оценок эффективности по каждому элементу и объекту в целом. Другими словами, величины рисков нарушения безопасности можно рассматривать как показатели эффективности существующей и эксплуатируемой на КВО системы обеспечения безопасности (СОБ).

Управление рисками определяется как совокупность процессов, связанных с идентификацией, анализом рисков и принятием решений, которые обеспечивают минимизацию отрицательных последствий наступления рисковых событий. Также принимается, что агрегированным показателем уровня защищенности объекта от всех видов потенциальных угроз является оценка уязвимости КВО, которая определяется на основе вычисления рисков нарушения безопасности объекта при наличии на нем СОБ и сравнении полученных значений с нормативно допустимыми. Для определения набора действий и процедур по решению выделенной выше задачи расчета рисков возможности возникновения критической ситуации на объекте, находящимся по воздействием разного типа угроз, целесообразно упрощенно представить предлагаемую методику.

Предлагаемая методология имеет ряд преимуществ, которые позволяют:

- однозначно проводить оценку эффективности существующего комплекса используемых средств защиты по каждой уязвимости;
- провести синтез комплекса средств защиты и выбор его в случае, когда величина оценки эффективности защиты (на основе риска возможности нарушения безопасности) меньше допустимой; при этом возможен выбор комплекса при различных условиях – минимум стоимости, максимум значения при заданной стоимости и т.д.;
- проводить моделирование появления критической ситуации и выработку (оценку) вариантов принятия возможных решений.

Необходимо отметить ориентацию предлагаемой методики на решение трех практических задач в рамках СППР.

Первая – оценка эффективности существующей, на момент проведения анализа, АСОБ на исследуемом КВО. Полученная количественная оценка риска нарушения безопасности является объективным основанием для принятия решений по мерам усиления защиты объекта. В результате выявляются наиболее слабые критические точки объекта (уязвимости) и необходимые меры по их ликвидации.

Вторая – определить состав и структуру АСОБ, обеспечивающей min ее стоимости при заданном уровне безопасности КВО. Решение этой задачи направлено на формирование оптимальной по стоимости АСОБ объекта при фиксированном уровне риска нарушения его безопасности.

Третья - определить состав и структуру АСОБ, обеспечивающей max безопасности КВО при заданной величине стоимости защиты. Решение этой задачи направлено на формирование оптимальной по эффективности системы защиты объекта при фиксированной стоимости его СОБ.

Результаты решения второй и третьей задачи позволяют сделать рекомендации по выбору средств защиты, обеспечивающих увеличение низких значений эффективности безопасности.

Соответственно, описание алгоритма реализации предлагаемой методики предусматривает наличие двух взаимосвязанных «ветвей»: первая – решение первой задачи; вторая – решение второй и третьей задачи.

Применение предлагаемого метода расчета эффективности обеспечения комплексной безопасности КВО при воздействия различного типа внешних и внутренних угроз требует использования большого объема заранее подготовленной информации. Для этого необходимо проведение достаточно трудоемких работ по её сбору и организации, что требует выполнения набора операций в рамках подготовительного этапа. Исходя из существа выполняемых операций и состава используемых данных проводится анализ всей информации с целью определения форм и вида ее представления на входе СППР, а также регламенты ее сбора, организации к ней доступа. Например, для проведения расчетов величины рисков (эффективности защиты) каждого критического элемента объекта необходимо из общей базы данных КВО выбрать и конкретизировать всю информацию, касающуюся:

- структуры и взаимодействия данного критического элемента КВО и его места в выполняемом КВО процессе;
- известных и потенциальных уязвимостей и критических точек (место проявления нарушения защиты уязвимости) элемента, характеристики всех средств наблюдения за ее состоянием;
- вида и формы показателей, характеризующих состояние уязвимости и/или критической точки, а также периодичности и форму их поступления на вход СППР;

– потенциальных угроз и способов их реализации для каждой уязвимости;

– профиля защиты, т.е. набора требований по защите каждой уязвимости от каждого средства реализации угрозы;

– средств защиты со всеми характеристиками (эффективность, стоимость, нормативная функция), используемых существующей АСОБ для защиты каждой уязвимости от каждого способа реализации угрозы; обязательно уточняется наличие дублирования и/или комбинации средств защиты на данной уязвимости. Мсл бЯ

Большое внимание должно быть уделено качеству, виду и формам представления результатов всех операций по расчету величин рисков возникновения критической ситуации на объекте.

Последней проблемой информационного обеспечения является задача собственной безопасности как АСОБ, так и СППР, включая проблему проверки достоверности и конфиденциальности информации, защиты ее от не санкционированного доступа, т.е. информационной безопасности на всех этапах работы.

Решение этих проблем жестко регламентируется имеющимися нормативными документами Правительства РФ, ФСБ РФ и ФСТЭК, что требует серьезного отношения к их решению.

Целесообразно формировать СППР в виде иерархической структуры, нижний уровень которой соответствует и обслуживает ЛПР участков, отделов и критических, но небольших элементов структуры КВО, средний – ЛПР цехов, служб и крупных критических элементов, а верхний – обслуживает руководство КВО. При этом все СППР информационно взаимосвязаны.

Накопленный опыт создания комплексной АСОБ, включающей в структуру СППР, показывает, что без специальной организационной структуры во главе с руководителем высшего управления КВО (не ниже заместителя генерального директора) задача является практически не выполнимой.

Следовательно, перед руководством КВО перед началом работ по модернизации АСОБ должен быть поставлен (и решен) вопрос об интеграции всех имеющихся на объекте подразделений по обеспечению безопасности в единую структуру с подчинением только одному руководителю.

Доклад отражает результаты работ по гранту РФФИ 15-07-01796.

Шевчик А.П., Мусаев А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)

КОГНИТИВИСТИКА: НОВЫЙ ВЫЗОВ ИНФОРМАЦИОННОЙ ЭРЫ

По мнению компетентных научных аналитиков и футурологов, 6-й технологический уклад, а вместе с ним и характер развития цивилизации, будут определяться информационными, био-, нано- и когнитивными технологиями. Когнитивистика представляет собой межотраслевой тренд, ориентированный на проблемы познания и мышления.

Развитие средств вычислительной техники и информатики позволило сместить цент тяжести когнитивных исследований с гуманитарных вопросов на задачи создания искусственного интеллекта и интеллектуальных приложений в самом широком диапазоне человеческой деятельности. В частности, рассматриваются возможности создания когнитивных ассистентов и саморазвивающихся робототехнических систем.

Особую роль когнитивистика играет в формировании новой образовательной парадигмы, когда традиционный подход накопления знаний заменяется новыми технологиями формирования креативного интеллекта, находящегося в состоянии перманентного самообразования.

Рузанова Н.С., Кудряшова С.В., Никольская Н.В.
Россия, г. Петрозаводск, Петрозаводский государственный университет,
Администрация Главы Республики Карелия

СОКРАЩЕНИЕ ЦИФРОВОГО НЕРАВЕНСТВА И ПРЕДОСТАВЛЕНИЕ ЭЛЕКТРОННЫХ УСЛУГ В РЕСПУБЛИКЕ КАРЕЛИЯ

В Республике Карелия на площади в 180,5 тыс. кв. км на сегодняшний день проживает 629,9 тыс. человек, удельный вес городского населения – 79,9. В 2015 году доля населения моложе трудоспособного возраста составляла 17,9%, трудоспособного возраста – 56,1%, старше трудоспособного возраста – 26%. В состав Республики Карелия входят 126 муниципальных образований, в том числе 16 муниципальных районов, 2 городских округа, 22 городских поселения и 86 сельских поселений. На территории республики расположены 775 населенных пунктов. Низкая плотность населения (3,5 человека на 1 квадратный километр), удаленность от столицы и районных центров, отсутствие развитых транспортных средств сделали актуальным использование интернета для решения социально-экономических задач в Карелии [1]. В настоящее время в Республике Карелия доступ к сети Интернет имеют более 82% домохозяйств. Число активных пользователей фиксированного широкополосного доступа к сети Интернет – 177,5 тыс. абонентов. Мобильной связью обеспечено 100 % городского населения и 97 % жителей сельских населенных пунктов.

С целью реализации положений закона «О связи» по проекту «Устранение цифрового неравенства» в рамках выполнения трехстороннего Соглашения (Минкомсвязь России, Правительство Республики Карелия, ПАО «Ростелеком») было определено 58 населенных пунктов, с численностью населения от 250 до 500 человек, на территории которых должны быть установлены точки доступа с цифровыми каналами связи, для построения сети передачи данных на скорости не менее 10 Мбит/с. В настоящее время обеспечены указанными точками доступа 56 населенных пунктов. По итогам работы в 2015 году количество населенных пунктов с низким уровнем развития телекоммуникационной инфраструктуры в Карелии снизилось с 151 до 70 населенных пунктов. Карельским филиалом ПАО «Ростелеком» в 2016 году дополнительно запланировано строительство волоконно-оптических линий связи к 14 населенным пунктам.

Во всех районах Карелии проводится модернизация существующего оборудования связи, что позволяет улучшить качество принимаемого сигнала, в определенной степени расширить существующую зону покрытия связью, а для ряда населенных пунктов расширить объем оказываемых услуг. К концу 2016 года ожидается увеличение зоны покрытия мобильной связью основных автодорог Республики Карелия.

Доля населенных пунктов с численностью свыше 1 тысячи человек с доступностью услуг мобильного широкополосного доступа составляет 86,5%. Для населенных пунктов численностью менее 1 тысячи человек доступность мобильного широкополосного доступа обеспечена всего для 21,5% населенных пунктов.

При этом основными проблемами развития сетей связи в поселениях являются: большая удалённость от магистралей операторов связи, высокая стоимость электрической энергии, отсутствие промышленного электричества или сложность подключения к электрическим сетям, а также малое количество потенциальных абонентов в поселениях.

Правительство РК активно проводит координирующую работу по взаимодействию операторов связи с целью развития в удалённых и труднодоступных населённых пунктах республики качественных и современных услуг связи, организации для населения доступа к сети Интернет и предоставления государственных и муниципальных услуг в электронной форме.

В Карелии создана региональная система межведомственного электронного взаимодействия (РСМЭВ РК) к которой подключены органы исполнительной власти - 21, органы местного самоуправления – 126, 78 подведомственных государственных и муниципальных учреждений. В республике на постоянной основе ведется работа по переводу государственных и муниципальных услуг в электронный вид. В результате чего увеличилась территориальная доступность для заявителей получения наиболее востребованных услуг в электронной форме, а также информированность граждан о возможности получения этих услуг [2]..

Через личный кабинет Портала государственных и муниципальных услуг Республики Карелия обеспечена возможность подачи заявлений в электронном виде более чем на 80 государственных и на 180 муниципальных услуг. Авторизация на Портале происходит посредством федеральной информационной системы «Единая система идентификации и аутентификации» (далее - ЕСИА), что позволяет пользователям порталов использовать один и тот же логин и пароль для федерального и регионального порталов. По состоянию на 1 сентября 2015 года через ЕСИА зарегистрировалось – 23,8% жителей республики, а по состоянию на 1 сентября 2016 года – 31,9%.

В целях повышения качества и доступности предоставления гражданам и организациям государственных и муниципальных услуг в Республике Карелия создана сеть многофункциональных центров предоставления государственных и муниципальных услуг (МФЦ). На сегодняшний день количество действующих в республике подразделений МФЦ составляет 18 офисов и 62 удаленных офиса (территориально обособленных структурных подразделений), в них открыто 194 окна обслуживания населения, а также 14 комфортабельных мобильных офиса. В рамках исполнения государственной программы «Доступная среда в Республике Карелия» в МФЦ обеспечены все необходимые условия для комфортного обслуживания населения. В том числе для оказания услуг инвалидам и малообеспеченным группам населения.

В настоящее время в МФЦ республики организовано предоставление 155 государственных и муниципальных услуг по принципу «одного окна»: 46 государственных услуг, предоставляемых территориальными управлениями федеральных органов исполнительной власти, государственных внебюджетных фондов; 83 государственных услуг, предоставляемых исполнительными органами государственной власти Республики Карелия; 26 муниципальных услуг. К концу 2016 года планируется организовать предоставление 182 государственных и муниципальных услуг.

В 2015 году в многофункциональных центрах в Республике Карелия зарегистрировано 212714 запросов граждан на предоставление государственных и муниципальных услуг. В настоящее время обеспечена возможность предоставления нескольких государственных и/или муниципальных услуг в рамках жизненных ситуаций посредством подачи заявителем единого заявления.

Значительная работа в Республике Карелия проводится по типизации однородных муниципальных услуг. Как показал проведенный анализ, однородные услуги муниципальных образований республики различаются по названию, по срокам предоставления услуги, по перечню

документов, по форме заявлений, по результату услуги, по возможности предоставления услуги через МФЦ. С технологической точки зрения такие муниципальные услуги считаются различными. Следовательно, на перевод в электронный вид каждой из таких услуг требуется выделение финансирования как на отдельную услугу. Кроме того, в случае актуализации переведенных в электронный вид услуг, вызванной изменением законодательства, необходимо внесение изменений по каждой из переведенных в электронный вид услуге. Типизация муниципальных услуг позволяет упростить этот процесс за счет тиражирования технологического решения на все однородные муниципальные услуги. Таким образом, отсутствие типизации муниципальных услуг влечет за собой не только временные потери, но и существенные финансовые затраты на перевод муниципальных услуг в электронный вид.

Для развития малого и среднего бизнеса большую роль играет фактор информированности об уровне развития территории. В целях предоставления услуги по информированию представителей малого и среднего бизнеса на территории республики Министерством экономического развития и промышленности РК с 2014 года ведутся работы по развитию информационной системы «Геопортал Республики Карелия». Данный проект включен в государственную программу РК «Информационное общество в Республике Карелия» на 2014-2020 годы. На данный момент в информационной системе «Геопортал Республики Карелия» в открытом доступе находится 15 тематических разделов, в которых содержится 57 слоёв с пространственными данными по таким направлениям, как инвестиции, связь, таможенная инфраструктура, энергетика, объекты ФЦП «Развитие Республики Карелия на период до 2020 года», транспорт, образование, здравоохранение, культура, социальная защита и ряд других.

В Республике остро стоят вопросы повышения качества и уровня оказания медицинской помощи населению и повышения доступности специализированной медицинской помощи [3].

На базе Республиканского медицинского информационно-аналитического центра создан региональный центр обработки данных системы здравоохранения, который позволяет использовать облачные технологии при создании и эксплуатации региональной информационной системы здравоохранения республики и для предоставления услуг населению.

В связи с тем, что все муниципальные учреждения здравоохранения сосредоточены в Петрозаводске, а также в районных центрах, наиболее востребованной услугой для жителей Карелия являются «Электронная запись на прием к врачу». За 2014 - 2016 годы данной услугой через «Единый медицинский портал Республики Карелия» воспользовалось более 10 % населения республики. Всего за три года гражданам оказано более 300 тысяч медицинских электронных услуг. В настоящее время в региональной информационной системе здравоохранения более 560 тысяч электронных медицинских карт пациентов.

Телемедицинская сеть Карелии охватывает все районы, городские округи республики, объединяет 24 телемедицинских пункта и центр телемедицины, созданный на базе Республиканской больницы им. В.А. Баранова.

В состав телемедицинской сети, входит радиологическая сеть, посредством которой в центральный архив медицинских изображений Республиканской больницы (в настоящее время в его базе данных более 6,5 млн.) передаются данные с 17 единиц цифрового диагностического оборудования, в том числе с томографов, расположенных в удаленных районах и городских округах республики (до 500 км).

На сегодняшний день ежегодно врачами республиканских лечебных учреждений проводится более 700 консультаций врачей центральных районных больниц, осуществляется не менее 100 консультаций по медицинским документам, включая диагностические изображения, в том числе видеофайлы.

Только за 1 квартал 2016 года специалистами республиканских больниц проведено 270 телемедицинских консультаций регионального уровня и организовано 25 консультаций со специалистами ведущих медицинских центров федерального уровня таких как РНЦХ им. Б.В. Петровского в г. Москве, Центр кардиохирургии ЛДЦ МИБС «Гамма-нож» г.Санкт-Петербург, ФГУ «Федеральный Центр сердца, крови и эндокринологии им. В. А. Алмазова», ФГУ «Российский кардиологический научно-производственный комплекс» г.Москва, НИИ нейрохирургии им. Н. Н. Бурденко, ВЦМК «Защита», Научный центр сердечно-сосудистой хирургии им. А. Н. Бакулева (Москва), РКИИТО им. Р. Р. Вредена, МНТК «Микрохирургия глаза» им. акад. С. Н. Федорова и др.

Кроме того, с помощью телерадиологической сети осуществляется круглосуточное дистанционное консультирование пациентов сосудистых центров. Оказание непосредственной информационно-консультационной помощи пациентам из удаленных поселений производится также через сайт Республиканской больницы им В.А.Баранова. На сегодняшний день сайт посетили около 500 тыс. пациентов, 80% - это жители Республики, 8%-жители зарубежья, 12% - жители регионов России.

Таким образом, в Карелии создана эффективная система межведомственного электронного взаимодействия (РСМЭВ РК), а также распределенная сеть многофункциональных центров, в результате чего увеличилась территориальная доступность для населения получения наиболее востребованных электронных услуг. Определяющим фактором в повышении качества и доступности квалифицированной медицинской помощи населению вне зависимости от места проживания становится развитие телемедицины.

Тимофеев Д.А.
Россия, г. Севастополь, Главное управление информатизации и связи г. Севастополя

ОСОБЕННОСТИ РАЗВИТИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В ГОРОДЕ СЕВАСТОПОЛЕ

Главное управление информатизации и связи города Севастополя (ГУИС) является уполномоченным органом исполнительной власти города Севастополя, проводящим государственную политику и осуществляющим управление в сфере информационных технологий, связи (в том числе почтовой), телекоммуникаций, информационной безопасности и обеспечения защиты персональных данных, развития информационного общества и формирования электронного правительства, геоинформационных и навигационных систем в городе Севастополе.

С момента вхождения города Севастополя и Республики Крым в состав Российской Федерации перед ГУИС встала задача в рамках своих полномочий принять необходимые меры по сохранению контроля над ситуацией с обеспечением региона связью: фиксированной электросвязью, мобильной, почтовой – на соответствующем уровне качества услуг.

В настоящее время ситуация стабилизировалась; удалось обеспечить следующее:

- ГУП Севтелеком – единый оператор стационарной телефонной связи – подведомственное предприятие ГУИС;
- ГУИС является единым архитектором информационных систем регионального уровня, с ГУИС согласовываются все технические задания, связанные с вопросами информатизации;
- запущена в работу инфраструктура, позволяющая развернуть и запустить в работу оказание услуг в электронном виде;
- благодаря ФЦП создана система РСМЭВ, в августе запущена в промышленную эксплуатацию;
- оказываются 25 приоритетных региональных услуг в электронном виде;
- создана единая программа информатизации региона на 2017-2019 г.г., выполнение которой позволит сделать вывод о наличии в регионе полноценно функционирующего комплекса электронного правительства;
- создана и запущена ОАО РНИЦ города Севастополя;
- строится СКС более чем в 40 разрозненных объектах;
- создается единая сеть передачи данных правительства города;
- внедряется единая система электронного документооборота.

В соответствии с распоряжением Правительства РФ от 03.12.2014 №2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город», для реализации единого системного подхода к обеспечению общественной безопасности, правопорядка и безопасности среды обитания в условиях сохранения высокого уровня рисков техногенного и природного характера, в г. Севастополе ведется активная работа по построению и развитию АПК «Безопасный город».

Постановлением Правительства Севастополя от 27.03.2015 № 224-ПП утверждена государственная программа «Создание системы обеспечения вызова экстренных оперативных служб по единому номеру «112» и элементов АПК «Безопасный город» на территории города Севастополя».

С июня 2015 года Система-112 работает в тестовом режиме.

Постановлением Правительства Севастополя от 11.03.2016 №155-ПП утверждена государственная программа «Построение и развитие аппаратно-программного комплекса «Безопасный город» на территории города Севастополя на 2016–2018 годы».

В 2016 году планируется завершение построение и запуск в промышленную эксплуатацию РНИС - государственной информационной системы, предназначенной для автоматизации процессов планирования, мониторинга, диспетчеризации и управления транспортом и критически важными объектами различного функционального назначения на территории города Севастополя;

Основными целями создания РНИС являются:

- обеспечение безопасности перевозок на территории города Севастополя, интеграция в Системы «Безопасный город» и «112»;
- повышение качества транспортных услуг, предоставляемых на территории города Севастополя, интеграция с системой Яндекс-транспорт;
- повышение эффективности контроля качества транспортных услуг, предоставляемых на территории города Севастополя;
- повышение экономической эффективности эксплуатации автомобильного транспорта различного назначения на территории города Севастополя;
- повышение эффективности процессов управления транспортным комплексом на территории города Севастополя;
- создание единого навигационно-информационного пространства на территории РФ.

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

КОНСТИТУЦИОННЫЙ ХАРАКТЕР ИНСТИТУТОВ ТАЙН

Накануне юбилейной, 25-й санкт-петербургской международной конференции «Региональная информатика (РИ-2016)» следует заметить, что четверть века назад, почти одновременно с первой, в Библиотеке Академии Наук, в Ленинграде проходила научная конференция «Свобода научной информации и охрана гостайн». Эта конференция в своей резолюции, направленной Председателям Верховных Советов России, Беларуси и Украины, призвала предпринять неотложные шаги по законодательному регулированию вопросов секретности, созданию, в тогда ещё единой стране, закона о государственной тайне. Вопросы законодательства о государственной тайне обсуждались также и в рамках первых конференций «Региональная информатика».

Российская история богата тайнами. Однако впервые понятие «тайна» появилось только в Конституции СССР 1936 г. Первыми видами тайны, получившими в нашей стране закрепление на конституционном уровне, стали тайна переписки и тайна голосования. Позже Конституции СССР 1977 г. добавила к ним тайну телефонных переговоров и телеграфных сообщений.

Вопрос о конституционном закреплении других видов тайны рассматривался в начале 90-х гг. в процессе разработки проекта новой российской Конституции. Так, например, в проекте Конституции, представленном Президентом Российской Федерации, присутствовали следующие виды тайны: «личная и семейная» «тайна переписки», «тайна почтовых, телеграфных, телефонных и иных сообщений». Проект Конституции, подготовленный Конституционной комиссией, предусматривал, что право на свободу мысли, слова, выражение мнений, а также право на свободный поиск, получение, производство и распространение информации могут быть ограничены федеральным законом. В этой связи следует заметить, что ещё в ноябре 1991 г. года Верховный Совет РСФСР принял Декларацию о правах и свободах человека и гражданина (Постановлением № 1920-1), статья 13(2) которой провозгласила: «Каждый имеет право искать, получать и свободно распространять информацию. Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности. Перечень сведений, составляющих государственную тайну, устанавливается законом». (Заметим, что служебная тайна среди перечисленных здесь не указана.)

В 1993 г. Президент Российской Федерации Б.Н. Ельцин вынес на рассмотрение комиссии Конституционного арбитража вопросы: «Необходимо ли вводить в Конституцию понятие “служебная тайна”?» и «Необходимо ли в Конституции устанавливать конкретный способ определения государственной тайны – перечень?». Комиссия Конституционного арбитража Конституционного совещания сочла, что понятие «служебная тайна» в Конституцию вводить не следует. Кроме того, Комиссия предложила свой вариант закрепления в Конституции нормы о государственной тайне: «Перечень сведений, составляющих государственную тайну, определяется федеральным законом». Первоначально предложенная формулировка гласила: «устанавливается федеральным законом исчерпывающим образом».

Как отмечают исследователи, в процессе подготовки Конституции Российской Федерации участники Конституционного совещания, стремились уйти от порочной практики советского периода, когда понятие государственной и служебной тайны произвольно трактовалось должностными лицами, а охрана государственных секретов служила поводом для необоснованного привлечения к уголовной ответственности и не позволяла гражданам своевременно получать необходимую информацию.

Закон Российской Федерации «О государственной тайне», принятый 21 июля 1993 г., отнёс часть сведений, ранее составлявших служебную тайну (это информация с грифом «секретно»), к категории государственной тайны. Разработчиками закона предполагалось, что институт служебной тайны также получит законодательное оформление, объектом его охраны станет, в частности, информация «для служебного пользования», информация, «полученная в результате исполнения служебных обязанностей» и др. Однако служебная тайна и по сей день и не получила должного правового оформления. Как отмечается в литературе, институт служебной тайны «повис в воздухе».

Уже в самом определении теоретико-правового понятия «тайна» в российской юридической науке можно встретить различные подходы. В рамках первого подхода тайна рассматривается в качестве информации, доступ к которой ограничен, другими словами, «тайна — это сведения», которые не являются общеизвестными и общедоступными. «Хрестоматийные» учёные-юристы говорят, что понятие «тайна» не сводимо к информации, иными словами, «тайна — это не информация, а особый правовой режим» — комплекс правовых средств», характеризующих сочетание взаимодействующих между собой, дозволений, запретов, а также позитивных обязываний, способствующих ограничению доступа и распространения определенных видов информации.

Представителями конституционного права тайна рассматривается, прежде всего, в качестве самостоятельного права, т. е. «права на тайну». Кроме того, тайна рассматривается в качестве гарантии реализации права.

В тексте действующей Конституции Российской Федерации (1993) понятие тайны встречается трижды: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (Ст. 23, ч. 1); «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» (Ст. 23, ч. 2); «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию. Перечень сведений, составляющих государственную тайну, определяется федеральным законом» (Ст. 29, ч. 4). (Попутно заметим, что таким образом, применительно к институту государственной тайны, уже постулируется перечневая модель засекречивания информации.)

Как отмечают исследователи, использование термина «государственная тайна» в Основном законе показывает осознание значимости этого института, а также служит основанием для отнесения защиты государственной тайны к конституционным ценностям. Конституционный Суд Российской Федерации в одном из своих постановлений, касающихся вопросов, связанных с ограничением прав граждан в целях обеспечения обороны страны и безопасности государства, указал, что «государство вправе относить те или иные сведения в области военной, экономической и других видов деятельности, распространение которых может нанести ущерб обороне страны и безопасности государства, к государственной тайне».

Право государства на тайну ограничивается конституционным требованием установить перечень сведений, которые могут составлять эту тайну, и закрепить его в форме федерального закона, который в соответствии с Конституцией Российской Федерации должен быть опубликован (Ст. 15, ч. 3). Ссылка на федеральный закон в данном случае не только соответствует требованию Конституции Российской Федерации о том, что права и свободы граждан могут ограничиваться только федеральным законом (Ст. 55, ч. 3), но и выступает гарантией от произвольного ограничения этих прав.

В заключение следует отметить, что закрепление указанных выше видов тайны в Конституции РФ создает своеобразную систему «сдержек и противовесов» деятельности человека и государства в информационной сфере. Придание конституционного статуса личной и семейной тайне, тайне сообщений способствует повышение степени свободы и защищенности личности. Конституционно-правовое содержание нормы о государственной тайне, в свою очередь, представляет собой, с одной стороны, ограничение субъективного права на поиск и распространение соответствующей информации, а, с другой — ограничение права субъекта государственной тайны (государства) на ограничение субъективных прав граждан.

Горбунова И.Б.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МУЗЫКАЛЬНОМ ОБРАЗОВАНИИ

На рубеже XX и XXI веков возникло новое направление в музыкальном творчестве и музыкальной педагогике, обусловленное быстрым развитием информационных технологий и электронных музыкальных инструментов (от простейших синтезаторов до мощных музыкальных компьютеров), новая междисциплинарная сфера профессиональной деятельности, связанная с созданием и применением специализированных музыкальных программно-аппаратных средств, требующая знаний и умений как в музыкальной сфере, так и в области информатики — музыкально-компьютерные технологии (МКТ). Данное понятие используется специалистами в различных музыкальных областях с начала XXI в. Во многих учебных заведениях мира музыкантам преподаются элементы МКТ (Институт исследований и координации акустики и музыки (IRCAM) при Центре имени Ж. Помпиду в Париже; CEMAMu (Centre d'Etudes Mathématiques et Automatique Musicales) в Париже, образованный Я. Ксенакисом; Центр компьютерных исследований музыки и акустики (CCRMA) Стенфордского университета; Центр музыкального эксперимента Калифорнийского университета в Сан-Диего; Научно-учебный центр МКТ (до 2006 г. — Вычислительный центр) Московской государственной консерватории им. П.И. Чайковского и др.); элементы музыкального программирования преподаются музыкантам в University of Hertfordshire, The University of Salford, Access to Music Ltd., Bedford College в Великобритании; Institut für Musik und Akustik (Zentrum für Kunst und Medientechnologie) в Германии; в филиалах University of California, Stanford University, New York University, Full Sail University (Флорида) в США и др.

Высокотехнологичная информационная образовательная среда требует поиска новых подходов и принципиально новых систем обучения. Инновационная музыкальная педагогика на современном этапе связана с применением МКТ — современного и эффективного средства повышения качества обучения музыкальному искусству на всех уровнях образовательного процесса. МКТ являются незаменимым инструментом образовательного процесса для различных социальных групп в приобщении к высокохудожественной музыкальной культуре, а также уникальной технологией

для реализации инклюзивного педагогического процесса при обучении людей с ограниченными возможностями здоровья.

Внедрение МКТ в образовательный процесс позволяет актуализировать новые возможности подготовки и переподготовки высококвалифицированных специалистов различных уровней, востребованных в современном обществе, а также раскроют перспективы в художественном образовании и музыкальной педагогике. В результате решения данной проблемы обоснованы пути реализации концепции музыкально-компьютерного педагогического образования, позволяющие качественно изменить уровень подготовки педагога-музыканта на различных этапах обучения, сформировать необходимый уровень его информационной компетенции.

В музыкальной практике большое распространение приобрел новый класс музыкальных инструментов, куда входят клавишные синтезаторы, рабочие станции, мультимедийные компьютеры и др. Построенные на основе цифровых технологий инструменты отличаются значительными выразительными ресурсами, что открывает широкие перспективы их применения в музыкальном образовании.

Комплексная инновационная образовательная система «Музыкально-компьютерные технологии в образовании педагога-музыканта», разработанная в учебно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А.И. Герцена, опирается на лучшие традиции отечественного классического музыкального образования, инновационный зарубежный опыт и современные МКТ и развивает как собственно музыкальное и информационно-технологическое образование, так и затрагивает социальные аспекты процесса информатизации художественного образования в целом.

Принципы, положенные в основу создания методической системы, являются базовыми для формирования новой предметной области в музыкально-педагогическом образовании, возможность появления которой обусловлена возникновением и развитием МКТ. Их существование является фундаментом для сформировавшихся на современном этапе видов профессиональной деятельности как музыкантов, работающих с МКТ (звукорежиссура, цифровая звукозапись, саунд-дизайн, саунд-продюсирование, исполнение на синтезаторах и MIDI-инструментах и пр.), так и программистов — разработчиков в области электронных музыкальных систем.

Методическая система обучения музыке построена на основе использования МКТ, специализированного программного обеспечения и специально организованного класса, а также на реализации инновационной по форме и методике групповой творческой форме проведения занятий.

Жигадло В.Э.
Россия, Санкт-Петербург, ООО «СимплГрупп»

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

Целью стратегии импортозамещения является обеспечение полной технологической независимости и информационной безопасности систем и продукции отечественных предприятий радиоэлектронной промышленности, средств связи и инфотелекоммуникаций, которая должна быть реализована комплексно по следующим направлениям: создание отечественных технологий разработки и производства аппаратуры и систем двойного назначения, (включая унифицированные отечественные узлы и устройства для применения в ОКР, САПР, производственное оборудование); создание отечественных технологий разработки и производства программного обеспечения; разработка и производство отечественной электронно-компонентной базы (под имеющиеся и планируемые отечественные проектные нормы, технологии и оборудование микроэлектроники); создание отечественных технологий производства перспективных телекоммуникационных аппаратно-программных средств и комплексов; разработка отечественных материалов для производства печатных узлов, приборов, автоматизированных рабочих мест, систем (стеклотекстолит, корпуса микросхем с жёсткими выводами, паяльные пасты, маски и др.).

Крайне важен данный вопрос при решении задач по реализации в Санкт-Петербурге инфраструктурных проектов в области информатизации.

В докладе дается системный анализ инфраструктурных проектов в области информатизации, таких как системы «Безопасный город», «Единый мониторинговый центр» (ЕМЦ), «Единый центр управления транспортом» (ЕЦУТ), АИС «ОБЖ», «Система 112». Рассматриваются ситемо-технические принципы их интеграции в единую систему на базе программно-аппаратных средств АИС «Smart Sity» («Интеллектуальный город») с учетом существующих возможностей по реализации базовых принципов импортозамещения.

Микони С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРОБЛЕМЫ КАЧЕСТВА РЕЙТИНГОВОГО ОЦЕНИВАНИЯ В УСЛОВИЯХ РЫНОЧНОЙ ЭКОНОМИКИ

Широкое распространение получили рейтинговые задачи. Они решаются с целью определения наиболее выгодных объектов вложения капитала, стимулирования организаций и работников, выявления престижных организаций (предприятий, университетов и пр.), отбора наиболее перспективных проектов, выбора выгодных товаров и услуг и т.д. Первые места в рейтингах сулят прямую или опосредованную экономическую выгоду.

В рейтинговых задачах важнейшей является проблема доверия результатам оценивания. Как известно в 2008-м году рейтинговые агентства «прозевали» начало мирового кризиса. Едва ли можно признать нормальным занижение рейтинговых оценок российских вузов в мировой табели о рангах. На стыке столетий невольно возникали следующие вопросы:

- почему наши профессора, уехавшие на Запад, учат их студентов?
- почему многие наши специалисты востребованы на Западе, не имея их дипломов?
- почему наши программисты побеждали коллег из престижных западных университетов, а наши школьники побеждали их на олимпиадах?
- почему многие изделия военного назначения до сих пор конкурентоспособны в мире?

Очевидно, что рейтинговые оценки также подвержены влиянию политики, как и другие аспекты жизнедеятельности, в то числе и спорт. Чёрным ящиком для нас являются методики рейтингования хозяйствующих субъектов по экономическим показателям такими рейтинговыми агентствами как Standard & Poor’s Rating Services (S&P), Moody’s Investors Service, Fitch Ratings. Нам неизвестно, какие экономические показатели они оценивают, и в какой степени. Учитывая тенденциозность западных оценок и зависимость от их агентств, Правительство РФ приняло решение об организации отечественного агентства по оцениванию хозяйствующих субъектов.

Если известные западные агентства нередко ошибаются непреднамеренно или умышленно в рейтинговых оценках различных объектов, то и отечественные организации не могут избежать таких ошибок. Причиной тому является высокая степень субъективизма, а, зачастую, и недостаточная квалификация разработчиков моделей многокритериального оценивания. Целью работы является анализ ошибок, возникающих на различных этапах оценивания, и предложение способов улучшения качества рейтинговых оценок.

РЕГИОНАЛЬНАЯ ПОЛИТИКА ИНФОРМАТИЗАЦИИ. ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО

Видясова Л.А.
Россия, Санкт-Петербург, Университет ИТМО

БАРЬЕРЫ НА ПУТИ РАЗВИТИЯ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ

В докладе представлены обобщенные результаты экспертного опроса, продолжающего серию исследований барьеров и перспектив развития технологий электронного правительства и электронного управления в России и странах ближнего зарубежья

Цель проведения экспертного опроса состояла в оценке факторов развития инструментов электронного участия в России, а также барьеров, препятствующих эффективному взаимодействию власти и общества. Исследование было проведено в августе-сентябре 2016 года Центром технологий электронного правительства Университета ИТМО.

Для проведения опроса была разработана онлайн анкета, доступ к которой был предоставлен группе экспертов, отобранных для участия в опросе. В ходе исследования организаторами был опрошен 41 эксперт из различных регионов. Среди экспертов были представители органов государственной власти (39%), научно-образовательных структур (31,7%), а также некоммерческих организаций и частных компаний (9,8% и 12,2%, соответственно).

В ходе опроса респондентам предлагалось оценить значимость возможных барьеров, препятствующих развитию инструментов электронного участия в России по следующей шкале: 1 – совсем не значимо, 2 – не очень значимо, 3 – нейтрально, 4 – скорее значимо, 5 – очень значимо. При обработке и интерпретации результатов были рассчитаны средние оценки, присвоенные экспертами каждому из барьеров.

По результатам исследования, наиболее значимыми барьерами, препятствующими развитию электронного участия в России, являются административные барьеры, а также отсутствие нормативно-правовой базы, регулирующей процедуры работы органов власти с электронными обращениями граждан (80,5% и 75,6% экспертов, соответственно, отметили их как «очень значимые» или «скорее значимые»). Также достаточно высоко эксперты оценили существование таких барьеров, как низкий уровень доверия к инструментам электронного участия среди граждан, недостаточное удобство использования существующих инструментов электронного участия (юзабилити характеристики), отсутствие личной/общественной выгоды от использования инструментов электронного участия и высокий уровень общественного и политического безразличия в обществе.

Наибольшее количество нейтральных оценок в данном перечне получил такой барьер, как «низкая информационная культура и компьютерная грамотность населения» (51,2%). Также, в основном, нейтрально оцениваются экспертами ужесточение ответственности за размещение в Интернете информации, имеющей, по мнению органов власти, некорректный характер и информационное неравенство.

Таким образом, исследование выявило наиболее острые проблемы административного, нормативного, социально-психологического характера, возникающие при использовании инструментов электронного участия в России.

Гордейчук А.А., Жук Д.В.
Россия, Санкт-Петербург, ООО «Интеллектуальные информационные системы», Университет ИТМО

ВОЗМОЖНОСТИ ТЕХНОЛОГИЙ С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

На рубеже 2015 – 2016 гг., произошел «перелом» в индустрии информационных технологий – основным вектором развития стали системы и платформы с элементами искусственного интеллекта, которые должны обеспечивать выполнение ряда повседневных задач, тем самым автоматизируя рутинные процессы.

В мире прочно устоялся ряд мнений относительно искусственного интеллекта машин. Людей давно занимают вопросы создания машин, наделенных искусственным интеллектом, с возможностью и ориентаций на повторение мыслительных и умственных способностей человека. После многих лет медленного, но устойчивого прогресса в этом направлении были созданы «умные» устройства, но они лишь помогают нам в решении повседневных задач, при этом не обладая интеллектом, а имитируя простоту взаимодействия за счет наличия дружественных интерфейсов. Тем не менее ряд прорывов

совершенных в последние год в научном мире и определенных областях промышленности возобновили интерес к искусственному интеллекту, что позволило привлечь дополнительные инвестиции к его разработке.

Сегодня применение искусственного интеллекта (в широком смысле) ограничивается решением конкретных задач. Несмотря на это, влияние ИИ на мире растет. Так, например, ИИ играет ключевую роль в системах управления транспортными средствами с частичным или же вообще без участия водителя, в беспилотных авиационных системах, которые трансформируют процессы глобальных перевозок и локальные логистические системы. Это затронет и множество других отраслей промышленности, изменения в которых происходят или ожидаются в ближайшие десятилетия. Эти процессы находят своё отражение в различных областях, в т.ч. и в государственном управлении: автоматизация процессов, электронные онлайн-консультанты по государственным услугам, обработка и анализ больших данных, системы поддержки принятия решений – всё эти системы являются в той или иной степени результатом изысканий в области искусственного интеллекта или же его предшественниками. ИИ обладает огромными возможностями упрощения бытовых вопросов в повседневной жизни, безопасность, регулирование, права, а также научных исследований и разработок, которые необходимо принять во внимание при эффективной интеграции этой технологии в государственных и частных секторов деятельности.

Как и любая трансформационная технология, искусственный интеллект несет в себе скрытые риски и ставит перед органами государственной власти и публичной политики сложные, а иногда и неразрешимые вопросы: сокращение рабочих мест, трансформация экономики, безопасность новых технологий и систем на их основе, юридическое регулирование и много другое. Например, разработка систем с элементами искусственного интеллекта требует создания новых высокотехнологичных рабочих мест для специалистов высокой квалификации, но при этом успешная реализация таких проектов приводит к частичному или полному сокращению рабочих мест в рамках той задачи, которую система решает. Системы с элементами ИИ мало изучены и полагаться на них полностью небезопасно из-за возможности непредсказуемости их поведения.

Серьезнейшими задачами, стоящими перед органами государственной власти и которые могут быть решены с помощью подобных систем являются агрегация данных из различных источников согласно фиксированной схеме, их накопление, последующая обработка и анализ полученных данных, а также предоставление государственных услуг населению. Именно поэтому во многих странах инициативы развития технологий ИИ вынесены на государственный уровень. Так например, в США создана правительственная комиссия по данному вопросу NSTC (National Science and Technology Council Subcommittee on Machine Learning and Artificial Intelligence), цель которой способствовать расширению сфер применения искусственного интеллекта и машинного обучения, для улучшения предоставления государственных услуг. Акцент сделан на городские системы и построение умных городов, системы поддержки психического и физического здоровья населения, социального обеспечения, уголовного правосудия, охраны окружающей среды и многие другие. Подобные инициативы появляются и в других странах, преимущественно – в Европе. Как показывает практика других стран, эффективное развитие подобных инициатив возможно только во взаимодействии органов государственной власти, экспертного сообщества и граждан при решении вопросов использования возможностей технологий искусственного интеллекта, и сферах применения этих технологий.

Горелик С.Л., Лещинский В.В., Иванов И.А., Малахов А.А.
Россия, Санкт-Петербург, Университет ИТМО
г. Москва, Аналитический центр при Правительстве Российской Федерации

ТРЕТЬЕ ПОКОЛЕНИЕ ТЕРРИТОРИАЛЬНЫХ ПАССАЖИРСКИХ ТРАНСПОРТНЫХ СИСТЕМ

Наше общество находится в начальной стадии очередной технологической революции. Основой этой революции стали мобильные средства коммуникации нового поколения, сочетающие в себе функции персонального идентификатора, средства голосовой и почтовой связи, информирования, оплаты, безопасности, контроля здоровья, мониторинга окружающего пространства и т.п. Дополнительно, эти устройства реализуют взаимодействие и обработку информации как участники интернета вещей (IoT).

Результатом новой технологической революции становится переход к новым технологиям в бизнес-процессах, подразумевают максимальный акцент на разработку специальных алгоритмов и программного обеспечения и использование изделий массового и крупносерийного производства в качестве базовых аппаратных решений. Такой подход уже начал широко использоваться в ряде отраслей, связанных со сферой услуг (например, такси, банковские и коммунальные услуги и др.) и дает существенную экономию инвестиционных и эксплуатационных затрат, расширяет функциональные возможности.

Системы управления транспортом, также испытывает необходимость перехода на новые технологии, потому что существующие уже не обеспечивают необходимого качества управления перевозками, уровня безопасности и комфорта для пассажиров, достоверности отчетных данных.

Охват граждан мобильными средствами коммуникации в РФ сегодня приближается к 90% от возможного уровня. Резко расширяется перечень приложений, в которых мобильные средства связи используются как идентификаторы, источники справочной информации, платежные инструменты и т.п. Два года назад приложения типа «UBER» обсуждались только в среде специалистов и бизнесменов. Сегодня более 50% граждан пользуются мобильными приложениями, причем на регулярной основе. «Юберизация» меняет структуру бизнеса, выводя на первые места тех, кто сокращает издержки и обеспечивает удобство пользователям. Пример такси должен стать наглядным уроком для консерваторов всех уровней.

Активное использование находящихся у пассажиров мобильных устройств, по нашим оценкам, может более чем вдвое снизить затраты на оборудование транспортных средств и предоставить новые услуги, которые сделают поездку на территориальных транспортных средствах более комфортной и выгодной для пассажира, более экономичной для перевозчика и безопасной для всех участников процесса перевозки.

Математическое обеспечение для предлагаемых решений по управлению, оплате проезда и отображению данных о текущем состоянии транспортных средств на маршруте, основано на технологии мониторинга сложных систем, опыте использования мобильных технологии в такси и других приложениях, оценке динамики потребительского спроса на мобильные услуги в различных отраслях. Решения обеспечивают существенное снижение затрат на бортовое оборудование, за счет использования относительно недорогих изделий массового производства и переноса основных задач на программное обеспечение, основанное на интеллектуальных алгоритмах. Существенное снижение затрат достигается также за счет активного использованием мобильных коммуникаторов, принадлежащих пользователям, на всех этапах перевозки: от планирования маршрута до оплаты проезда и получения инструкций по перемещению для достижению промежуточных и конечной целей поездки. Глубокая интеграция систем автоматизированного управления транспортной работой, оплаты проезда и информационных сервисов обеспечивает более высокую достоверность отчетных данных. Особенно эффективна предлагаемая технология для мультимодальных перевозок с учетом метро и пригородного ЖД транспорта, когда необходимо обеспечить максимальную стыковку расписаний и сократить время поездки для пассажиров. К этим факторам очень чувствителен такой важный показатель качества перевозки, как удовлетворенность пассажиров. Можно классифицировать этот направление как создание третьего поколения городского пассажирского транспорта.

В докладе представлены подходы, обеспечивающие плавный переход пассажирской транспортной системы на третье поколение. Предлагается постепенное замещение и частичное включение в новую систему за счет доработки программного обеспечения, без его полной замены, что резко сократит расходы и снизит проблемы переходного периода.

Григорьев Л.Ю., Кононова О.В.
Россия, Санкт-Петербург, Бизнес инжиниринг групп, Университет ИТМО

МОДЕЛИРОВАНИЕ СИСТЕМ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ НА ОСНОВЕ АРХИТЕКТУРНО-ИНЖЕНЕРНЫЙ ПОДХОДА

Современные информационные и мобильные технологии поменяли ранее сложившуюся природу отношений между государством и гражданским обществом. Сегодня не только бизнес-организации, институты гражданского общества, но и отдельные граждане ожидают доступности разнообразных электронных сервисов в круглосуточном режиме. С управленческой точки зрения наиболее общее представление о государстве, также как и об организации, можно получить на основе моделирования и анализа деятельности.

Государство формирует управляющие воздействия в соответствии с предполагаемым будущим на основе некоторой модели развития. Модель развития подразумевает наличие «плановых» трансформаций, сохранение и развитие способностей и ценностей, приобретенных в результате этих трансформаций, что невозможно в отсутствии видения общей архитектуры системы. Все это позволяет утверждать, что условием поступательного развития современной системы государственного управления, электронного государства является использование моделирования деятельности для построения адаптивных структур, систем, форм и моделей целевого управления сложными системами.

Средствами борьбы со сложностью систем государственного управления являются стандартизация и моделирование. Моделирование деятельности по оказанию государственных услуг сопоставимо с моделированием деятельности предприятия. Применение моделирования позволяет повысить надежность и результативность государственных услуг (с точки зрения потребителя) и эффективность использования ресурсов. Эффективность достигается, прежде всего, за счет

стандартизации деятельности органов государственной власти на всех уровнях управления и оптимизации процессов межведомственного взаимодействия подчиненных им структур.

Практики моделирования процессов достаточно хорошо прижилась в российских компаниях: имеются специалисты, методики и инструменты. Однако, как показывает опыт, наибольшие проблемы при моделировании деятельности органов государственной власти связаны не с описанием процессов, а с формированием их состава и структуры, иными словами с архитектурой.

Целью работы является описание архитектурно-инженерного подхода к моделированию системы государственного управления (архитектурный бизнес-инжиниринг – АБИ). Архитектурный бизнес инжиниринг – это проектирование и трансформация предприятия на основе точной модели его деятельности. Новизна подхода состоит в комплексном использовании архитектурного и инженерного подходов. Первый обеспечивает понятность, системность и повторяемость элементов модели. Второй предлагает использовать методы технического системного инжиниринга. В этом случае система государственного управления проектируется как техническая система.

Применение предлагаемого подхода в полной мере оправдано для моделирования архитектуры электронного государства. Таким образом, моделирование системы государственного управления на основе оптимизированных стандартных шаблонов элементов деятельности должно положительно сказываться на качестве предоставляемых государственных услуг.

Совершенствование основных положений Архитектурного бизнес-инжиниринга (АБИ) происходит на основе практического применения и с учетом результатов современных исследований в области M&S и архитектуры предприятия. АБИ позволяет строить архитектуру и моделировать отдельные виды деятельности органов государственного управления всех уровней (федеральных, региональных, муниципальных) в соответствии с их целевым назначением. К преимуществам подхода АБИ следует отнести следующие:

- АБИ базируется на референтом матричном каркасе, задающим стандарты деятельности во всех существенных областях, что существенно повышает качество создаваемой модели органов госуправления.
- АБИ позволяет сократить время моделирования системы государственного управления за счет особой организации модели, построенной из стандартизированных элементов.
- АБИ является отечественным подходом, разработанным в России с учетом Российских реалий и соответственно полностью соответствует программе импортозамещения.

Общий рост эффективности применения АБИ достигается также за счет связанности изменений. Совершенствуя деятельность в определенной стандартизированной области можно улучшать деятельность во всех других, на которые распространяется стандарт.

Развитием подхода может стать интеграция методологии АБИ, основным объектом которой является бизнес-архитектура, и методологией The Open Group Architecture Framework (TOGAF®). Эффект от интеграции будет достигнут за счет использования и адаптации Architecture Development Method (ADM) для моделирования бизнес-архитектуры.

Зенченкова К.С., Чугунов А.В.
Россия, Санкт-Петербург, Университет ИТМО,
НП «Партнерство для развития информационного общества на Северо - Западе»

СИСТЕМА МОНИТОРИНГА ПОРТАЛОВ ЭЛЕКТРОННОГО УЧАСТИЯ КАК ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО СОПРОВОЖДЕНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВЛАСТИ

В настоящее время в России достаточно активно развиваются методы и технологии «электронного участия», которые позволяют органам управления и общественным движениям организовать канал «обратной связи» по вопросам решения городских проблем. Например, создаются информационные ресурсы, предназначенные для подачи «электронных жалоб» на благоустройство и городские проблемы. К таким порталам можно отнести «Наш Санкт-Петербург», «Красивый Петербург» «Наш город» (Москва), «РосЯма», «Сердитый гражданин» и многие другие. Все эти порталы позволяют подать жалобу на различные темы, связанные с благоустройством и развитием территорий. Создателями одних ресурсов являются городские власти, других – волонтерские движения. Большое количество подобных электронных площадок развивает систему электронного участия граждан и содействует развитию системы взаимодействия власти и общества.

Порталы электронного участия в ходе своего функционирования создают значительный объем информации, который может быть использован для проведения социальных исследований и определения спектра актуальных проблем, которые волнуют граждан. В 2015 году Университетом ИТМО, совместно с Партнерством для развития информационного общества на Северо-западе России реализована первая версия системы мониторинга порталов электронного участия (http://analytics.egov.ifmo.ru/).

Система мониторинга порталов электронного участия (далее Система) предназначена для сбора информации о динамике функционирования подключенных к ней информационных ресурсов и

применяется для анализа, фильтрации, навигации и отображения данных в целях мониторинга и проведения научных и аналитических исследований. Реализации Системы предшествовала серия исследований, в ходе которых были выделены два основных вида ресурсов: порталы для подачи инициатив (такие, как «Российская общественная инициатива», «Change.org и др.) и порталы городского участия (такие, как «Красивый Петербург», «Наш Санкт-Петербург», «Сердитый гражданин» и др.). Имеется также третий тип ресурсов – дискуссионные площадки, однако этого рода сайты (и разделы сайтов) представляют собой слабоформализованные объекты анализа и на данном этапе не предусмотрены для подключения к системе автоматизированного мониторинга.

Система начала функционировать в начале 2015 года, когда был запущен модуль визуализации данных портала «Российская общественная инициатива». Осенью 2015 года начались работы по подключению порталов «Красивый Петербург» и «Наш Петербург». После анализа вышеуказанных порталов было создано техническое задание для программирования модуля Системы.

В докладе представлены результаты работы с порталами городского участия, в частности описана структура программного модуля и базы данных, которые были спроектированы для подключения к Системе порталов «Наш Санкт-Петербург» и «Красивый Петербург».

В результате можно констатировать, что Система, разработанная в Университете ИТМО (Центр технологий электронного правительства и кафедра управления государственными информационными системами ФТМИ), позволяет аккумулировать данные об электронных заявках граждан, которые озабочены определенными проблемами в сфере городского хозяйства. Тем самым создан аналитический инструмент, позволяющий отследить, как по отдельной проблеме, так и по группе проблем ряд параметров, свидетельствующих о состоянии работы с обращениями граждан. Это позволяет использовать созданную Систему для научных и аналитических исследований, а также для мониторинга эффективности деятельности органов власти и структур, занимающихся управлением городским хозяйством.

Дмитрова О.А.
Россия, Санкт-Петербург, Университет ИТМО

ПОДХОД К ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМУ ОБЕСПЕЧЕНИЮ АНТИНАРКОТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА

В докладе представлены результаты первого этапа исследования социально-культурных и экономических факторов наркотизации населения. Согласно определению, предложенному Г.В. Шевченко, наркотизация представляет собой «процесс интеграции индивида в наркотическую среду, функционирующую в обществе, в результате активизации взаимодействия факторов, способствующих развитию злоупотребления психоактивными веществами и наркотическими средствами двух уровней: личностного и социальной среды».

В основе наркотизма лежит комплекс причин, основную роль среди которых играют именно социальные, выражающиеся в негативном влиянии социального окружения.

Социальный характер наркотизма требует концентрации усилий в следующих направлениях:

- социально-управленческих действий, направленных на устранение причин распространения наркомании и наркотизма путем регулирования системы социальных отношений;
- организации социальной работы с молодежью, ориентированной на содействие последней в решении жизненных проблем;
- административных решений и действий, включающих в себя ограничение наркобизнеса и наркопреступности;
- воспитание молодых людей, позволяющее сформировать в их сознании антинаркотические ценности и убеждения.

В основе противодействия наркотизации населения должны лежать точные представления об исследуемом явлении. В том числе важной задачей является исследование особенностей и специфики институциональной картины наркотизации. Построение модели взаимодействия акторов данного процесса может помочь как исследователям, так и практикам (структурам, занимающихся профилактикой распространения наркотиков).

Мониторинг и анализ ситуации с наркотиками в данный момент является одним из самых актуальных вопросов государственной политики и деятельности по профилактике и борьбе с незаконным оборотом наркотиков и наркоманией.

В Санкт-Петербурге мониторинг наркоситуации осуществляется с применением автоматизированной информационной системы «Антинар СПб».

АИС «Антинар СПб» - автоматизированная система, ориентированная на комплексный анализ наркоситуации во всех сферах жизнедеятельности города, выявление важнейших тенденций и закономерностей ее развития, информационно-аналитическую поддержку процесса принятия управленческих решений руководством Санкт-Петербурга.

В системе сформирована единая межведомственная БД по показателям наркоситуации, обеспечивающая возможность их анализа, сопоставления и прогноза. Работа с данными по показателям наркоситуации, поступившим из разных ведомств, позволяет не только увидеть картину в целом, но и выявлять скрытые процессы или намечающиеся тенденции, изучать состояние и динамику наркоситуации, а также ее отдельные составляющие.

Наличие межведомственной системы позволяет координировать деятельность соответствующих исполнительных органов государственной власти с учетом общегородских задач. В то же время система не в состоянии обеспечить точное представление о наркоситуации в регионе в связи с тем, что проблема наркомании имеет специфические черты и характеризуется высокой латентностью (наличием значительной доли скрытых потребителей наркотиков). Для оценивания этой величины используется коэффициент латентности. Коэффициент латентности вычисляется как отношение численности фактического числа потребителей наркотиков к численности состоящих на государственном учете наркоманов. В Санкт-Петербурге он колеблется от 8 до 10 для потребителей тяжелых наркотиков и от 40 до 50 для потребителей легких наркотиков.

Таким образом исследование проблемы наркомании невозможно без мониторинга социальных сетей и Интернет-СМИ, т.к. почти любое событие отражено в Интернете. Кроме того необходимым компонентом мониторинга являются социологические исследования и мнения экспертов по широкому кругу вопросов наркоситуации.

В рамках программы исследования предполагается сочетать данные, получаемые из государственных информационных систем, с информацией мониторинга социальных медиа с информацией социологических исследований. Исследовательский проект осуществляется в сотрудничестве с СПб ГУП «Санкт-Петербургский информационно-аналитический центр».

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ МЕГАПОЛИСОМ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА

В настоящее время широко обсуждаются решения по созданию «интеллектуальных» («умных») систем управления крупными городами. На практике во многих регионах интенсивно внедряются различные системы автоматизации и управления различными аспектами жизнедеятельности: управление уличным освещением («умное городское освещение»), управление безопасностью на дорогах («Безопасный город»), обеспечение безопасности жизнедеятельности (АИС «КСОБЖН») и т.д.

В России все чаще, наряду с системами «Безопасный город», говорят и о системах «Умного города».

"Безопасный город" - это программа установки на улицах российских городов автоматизированных систем наблюдения, контроля и управления, предназначенных для нужд МЧС, полиции и других экстренных служб.

«Умный город» – это комплекс организационных мероприятий и программно-технических решений, направленных на устойчивое социально-экономическое развитие города, создание высокотехнологичной наукоемкой экономики, эффективное использование всех видов ресурсов (электричество, вода, газ/тепло, пространство, время) и создающих условия для удобного пребывания в городе, комфортного проживания и ведения бизнеса. «Умный город», который сочетает в себе технологии энергоснабжения, автоматизированного управления, позволяет обеспечить комфорт и безопасность его жителей. Технологии «умного города» касаются различных сфер городской жизни и инфраструктуры: транспорта, городского хозяйства, градостроительной политики, экологии, медицины, образования, туризма, сферы услуг.

В докладе рассматриваются особенности реализации таких городских информационных программ, как «Безопасный город», АИС «ОБЖ», РЦУТ и предлагается подход к их интеграции на базе решений «Умный город».

Кондратьев В.В.
Россия, Санкт-Петербург, Университет ИТМО

ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

В настоящее время сведения, отнесенные к категории ограниченного доступа, разделяются на шестьдесят четыре категории на основании восьмидесяти пяти нормативно правовых актов РФ, из которых семнадцать впервые введены за последние пять лет. К информации «ограниченного доступа» в современном мире тесно примыкает информация «ограниченного распространения». В статье 4 закона РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» указано семь категорий информации, распространение которых не допускается в СМИ. Эта статья редактировалась двенадцатью федеральными законами, четыре из которых введены за последние 5

лет. К числу нормативно правовых актов, регулирующих информационные потоки в автоматизированных системах, относится и Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Этот закон за 10 лет своего существования редактировался десять раз за последние 6 лет.

В последнее несколько лет получили стремительное развитие социальные сети, которые могут оказывать огромное влияние даже на основы государственного управления. Вовлечение в них практически всех слоев общества и социальных групп позволяет накапливать, анализировать и использовать огромные объемы персональных данных всех социально активных групп населения. Эти данные касаются не только и не столько их персональных данных в самом широком толковании этого понятия ФЗ «О персональных данных» от 27.07.2006 № 152-ФЗ (любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу), но и данные, касающиеся психологических особенностей, морально-волевых и этических качеств и политических предпочтений. Это дает возможность участия этих социальных сетей в самых разнообразных коммерческих операциях с личными данными, включая и политическое влияние на общество, в том числе манипулируя общественным настроением на основе массовой организации аффективного участия граждан или для вовлечения их в акции экстремисткой направленности.

Кроме очевидного всем добровольного обмена информацией пользователей сети в интернете, существует и взаимное проникновение интернет-сетей в других каналы обмена, накопления и хранения информации. Так, например, Санкт-Петербургское государственное казенное учреждение «Городской мониторинговый центр» во всех 18 районах Санкт-Петербурга установил более 16 тысяч камер. В их поле зрения – сложные перекрёстки, оживлённые магистрали, наиболее людные места и жилые массивы. Только в 2015 году в Петербурге «ГМЦ» установил около 12 тысяч видеокамер, обмен информацией в которых происходит в сети интернет. Огромное количество видеокамер и других средств наблюдения за повседневной жизнью населения Санкт-Петербурга (например, геолокация устройств GSM и Wi-Fi сетей, мониторинг поисковых запросов, платежной информации) имеется в распоряжении и других государственных и негосударственных учреждений, в том числе коммерческих. Нельзя недооценивать и крупные поисковые и новостные сети и агрегаторы, которые тоже собирают, анализируют общественное мнение и могут оказывать значительное влияние на него. Большое распространение получили личные видеорегистраторы, web-камеры и смартфоны с видеозаписью, часть видеоматериалов которых переносится в социальные сети и предоставляется на общественное ознакомление.

Таким образом, можно сделать вывод, что в российском сегменте сети интернет неконтролируемо циркулирует любая информация, представляющая интерес для крупных коммерческих и политических структур всего мира, и эту информацию могут контролировать и использовать в своих целях любые крупные коммерческие, политические и криминальные структуры и отдельные личности.

Резюмируя вышесказанное, можно сформулировать следующие предложения:

1. Приступить к разработке Информационного Кодекса как кодифицированного нормативно-правового акта регулирования информационных отношений, в том числе как нормы частного права.
2. Вывести сведения с грифом «секретно» из области государственной тайны и использовать этот гриф как «служебная тайна», в том числе «адвокатская», «нотариальная», «банковская», «персональные данные» и т.д. Перечень и порядок защиты такой информации определяет руководитель организации и несет ответственность за ее безопасность.
3. Сохранить систему лицензирования для гостайны на информационные отношения служебной тайны.

Коршунов И.Л., Левкин И.М., Микадзе С.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

О СОЗДАНИИ ИССЛЕДОВАТЕЛЬСКОГО РЕГИОНАЛЬНОГО СИТУАЦИОННОГО ЦЕНТРА МОНИТОРИНГА КОНКУРЕНТНОЙ ОБСТАНОВКИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Развитие информационного общества ставит новые задачи перед подготовкой кадров в области информационных технологий. В частности, в экономическом вузе ИТ-кафедры, по нашему мнению, должны сосредоточить внимание на разработке и внедрении новых информационных технологий в экономику, а также на подготовке экономистов, владеющих этими технологиями.

В свою очередь, экономический вуз должен строить свой учебный процесс в тесном взаимодействии с задачами, стоящими перед предприятиями, что позволит готовить востребованных выпускников. Как вариант соединения усилий вуза и бизнеса в процессе подготовки квалифицированных кадров для экономики, в Санкт-Петербургском государственном экономическом университете рассматривается создание Исследовательского регионального ситуационного центра мониторинга конкурентной обстановки в информационной сфере (далее – Центр). Основной целью этого Центра должна стать оценка текущей конкурентной обстановки в регионе в сфере

информационных систем и технологий и прогнозирование ее развития в интересах бизнеса. В наличии такого Центра заинтересованы представители ряда предприятий. Задачи Центра можно сформулировать следующим образом:

- добывание (сбор) и обработка информации о хозяйствующих субъектах, функционирующих в сфере информационных систем и технологий;
- оценка конкурентоспособности, сильных и слабых сторон отечественных и зарубежных информационных продуктов и услуг по запросу предприятий бизнеса;
- предоставление услуг по оценке силы и намерений конкурентов, потребителей и поставщиков;
- моделирование и вскрытие конкурентных угроз предприятиям бизнеса;
- создание информационной базы по существующим и перспективным разработкам в сфере информационных систем и технологий, ведущим специалистам и системам их подготовки в регионе, России и за рубежом для нужд предприятий бизнеса;
- определение востребованности разрабатываемых информационных продуктов и услуг в различных сферах социально-экономической деятельности по запросам предприятий;
- оценка лояльности персонала внутри хозяйствующего субъекта и динамики ее изменения, выявление центров напряженности;
- вскрытие фальсифицированных данных, поступающих в высшие эшелоны управления хозяйствующих субъектов от собственных сотрудников и исключение дезинформации высшего руководства;
- предоставление услуг по разработке предложений по повышению эффективности хозяйствующих субъектов.

Активное участие в деятельности Центра должны принять ИТ-кафедры университета, обеспечивая информационную поддержку его работы. Кроме того, кафедре информационных систем и технологий, реализующей образовательные программы по направлениям 38.03.05 «Бизнес-информатика» и 09.03.02 «Информационные системы и технологии», целесообразно рассмотреть вопрос о введении новых профилей. Подготовка выпускников по новым профилям могла бы базироваться на работе Центра.

В связи с принятием ФГОС ВО 3+ по направлению 38.03.05 «Бизнес-информатика» (август 2016 г.) целесообразно переработать основную образовательную программу по данному направлению в соответствии с современным развитием науки в области информационных технологий и экономики, а также специфики нашего университета и создать новый профиль «Деловая разведка». В соответствии с определением «Деловая разведка означает совокупность мероприятий осуществляемых с целью добывания информации о конкурентах, условиях предпринимательской деятельности, конъюнктуре рынка, основных тенденциях бизнеса, возможных рисках и т.п. в интересах увеличения доходов, избегания неоправданных расходов, сохранения положение на рынке товаров, работ, услуг или получения иной коммерческой выгоды» [1]. Таким образом, подготовка специалистов по деловой разведке в рамках направления «Бизнес-информатика» вполне оправдана.

В условиях развития информационного общества в деловой разведке резко возрос объем информации, которую необходимо переработать для получения необходимых данных о конкурентах. Кроме того, резко усложнилась конкурентная обстановка. Она приобрела глобальный характер, стала более динамичной и менее прогнозируемой. В этих условиях требуются новые подходы к организации процесса добывания и обработки информации о конкурентах. В сложившейся ситуации нужны специалисты, которые способны разрабатывать новые информационные технологии (инструменты) для специалистов по деловой разведке. В связи с этим, введение нового профиля «Информационные технологии в деловой разведке» для направления 09.03.02 «Информационные системы и технологии» считаем вполне обоснованным.

Как продолжение обучения по двум указанным выше профилям подготовки бакалавров на следующем уровне мы предлагаем открыть магистерскую программу «Информационно-технологическая деятельность и деловая разведка» по направлению 09.04.02 «Информационные системы и технологии».

Реализация указанных в докладе предложений, по нашему мнению, позволит объединить усилия экономического вуза и бизнеса в подготовке квалифицированных кадров.

Лавреш И.И.
Россия, Республика Коми, г. Сыктывкар, ГАУ РК «Центр информационных технологий

О СТРАТЕГИИ ИМПОРТОЗАМЕЩЕНИЯ В СФЕРЕ ИТ РЕСПУБЛИКИ КОМИ

Стратегия импортозамещения в сфере информационных технологий Республики Коми разработана для формирования комплексного подхода к решению задач по замещению ИКТ в Республике Коми, а его реализация направлена на обеспечение мер по поддержке отечественных разработчиков ИКТ и обеспечению информационно-коммуникационной безопасности региона от влияния внешнеэкономических и внешнеполитических факторов.

Цели Стратегии импортозамещения мы рассматриваются на двух уровнях: глобальном и локальном.

Под глобальными целями понимаются стратегические цели уровня государственного управления в процессе импортозамещения, а именно:

Обеспечение государственной политики информационной безопасности. Данная цель возникает ввиду того факта, что использование импортной техники и привлечение иностранных фирм при создании информационных систем (ресурсов) повышает вероятность несанкционированного доступа к информации, риск осуществления различных диверсий и усугубляет зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, программного обеспечения.

В качестве глобальной цели номер два можно выделить развитие ИТ-отрасли России. Реализация мероприятий по импортозамещению в сфере информационных технологий способствует созданию благоприятной среды для развития российской ИТ-отрасли за счет создания дополнительных внешнеторговых, технических, административных и других стимулов. При этом есть понимание, что продукты ИТ-отрасли имеют высокую добавленную стоимость, что повлечет рост экономики России в целом.

Под локальными (или региональными) целями мы подразумеваем стратегические цели регионального уровня, которые регион достигает, обеспечивая процесс достижения глобальных целей.

По аналогии с целями Стратегии импортозамещения в сфере ИТ ее задачи также рассматриваются для двух уровней: федерального и регионального.

Необходимо понимать, что импортозамещение в сфере ИТ – процесс, который может быть реализован только общими усилиями всех заинтересованных лиц.

Для того чтобы импортозамещение было эффективным и способствовало достижению поставленных целей и заявленных задач, необходимо также сформировать принципы импортозамещения в сфере ИТ и следовать им в процессе реализации импотозамещения. К ним относятся:

- обеспечение работоспособности всех контуров ИКТ;
- экономическая целесообразность;
- рациональное импортозамещение.

В докладе представлена методика и матрица импортозамещения, позволяющая определить, на какие объекты ИТ-инфраструктуры повлияет замена того или иного ИТ-элемента, выявить масштабы, трудоемкость и экономическую эффективность импортозамещения рассматриваемого элемента. Реализация методики должна привести к формированию конечного плана мероприятий с указанием сроков, ответственных и участников импортозамещения в сфере ИТ.

В результате реализации Стратегии мы надеемся осуществить меры по обеспечению информационной безопасности и защите от кибердиверсий сферы ИКТ в Республике Коми, для всех секторов экономики и государственного управления осуществить переход на замещенные решения, ввести стандарты, правила использования и перечни конфигурационных элементов ИКТ.

Мисников Ю.Г., Филатова О.Г.
Республика Беларусь, г. Минск,
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный университет

КОНЦЕПЦИЯ СОЗДАНИЯ ИНСТРУМЕНТАРИЯ ОБРАТНОЙ СВЯЗИ ДЛЯ ПОРТАЛА ОБЩЕСТВЕННОЙ ПАЛАТЫ САНКТ-ПЕТЕРБУРГА

Наблюдаемый в последнее десятилетие по всему миру заметный рост активности граждан в области публичной жизни и политики в значительной степени определяется широкими возможностями доступа с интернету в целом и интерактивным потенциалом социальных сетей в особенности.

Вместе с тем, задача вовлечения в общественный диалог через, например, публичные обсуждения и консультации с помощью новых медиа является трудной задачей, по крайней мере в отношении адекватного понимания и интерпретации многочисленных мнений граждан, выражаемых в онлайновой среде, с одной стороны, и обеспечения минимального уровня доверия граждан к такому механизму общения власти и общества – с другой. Существующие инструменты анализа комментариев, размещаемые гражданами, например, в социальных сетях, часто ограничиваются выявлением общей тональности (позитивной или негативной) сообщений или доминирующих тем (в зависимости от частоты упоминания по ключевым словам), в то время как смысл сообщений остается не до конца понятым. Многие платформы проведения дискуссий и общественного диалога нацелены на демонстрацию аргументов и направлены на узкую группу экспертов, чем обычных граждан, и, как результат, не используются в реальной жизни. Также их главным недостатком является отсутствие связи с проблематикой принятия решений.

Есть большая вероятность, что быстро развивающиеся технологии искусственного интеллекта (как, например, глубинное машинное обучение) будут способны в недалеком будущем решать содержательно-смысловые задачи тестов сообщений в применении к сфере управления, но пока приемлемых решений в этой области не существует. Кроме того, недостаточно просто создать инструменты вовлечения граждан. Важно заинтересовать их выражать свое мнение, что не всегда удается реализовать на практике; например, на технически хорошо реализованных платформах обсуждения новых законодательных инициатив в России (https://regulation.gov.ru/projects) и Казахстане (https://legalacts.egov.kz/application/viewcards) практически отсутствуют комментарии. Так, по состоянию на июль 2016, всего 5 документов из 1 тыс. были прокомментированы на официальном сайте размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения. В свою очередь, проект «Активный Гражданин» в Москве отдает предпочтение рейтинговому голосованию как форме обсуждения, рассматривая отданные голоса как мнения по выбору одного из предложенных вариантов, что не совсем верно, так как такой подход оперирует понятием «мнение» в узком смысле, исключая его смысловую составляющую. Хотя такой подход также имеет право на существование.

Тем не менее, в целом недостаточная активность граждан на официальных платформах вовлечения объясняется не столько отсутствием их интереса к проблемам общества (активность граждан в обсуждении таких проблем в социальных сетях свидетельствует об обратном) и предлагаемым решениям, сколько различным пониманием самого процесса обсуждения, роли мнений, позиций в этом процессе и их содержательной оценке. Анализ существующей практики показывает, что люди, как правило, понимают, что не все их мнения власть сможет принять во внимание. Их волнует прежде всего прозрачность самого процесса обсуждения и реакция власти на их вклад (учитывая потраченное время на размещение комментариев); иными словами, для людей важно понимание того, что их мнения адекватно проанализированы, качественно оценены и объяснены, так как самим участникам дискуссий не всегда видна более широкая картина значимости обсуждаемых вопросов и то, как последние пересекаются друг с другом на более высоком уровне агрегации.

Исследования также показывают, что в равной (если не в большей) степени людей интересует реакция на их мнения других граждан, а не только власти. Очень часто именно дискуссии среди самих граждан по предложенной проблематике позволяют выявить все многообразие и глубину коллективного, не только частного, мнения. В этой связи предлагается построить систему обратной связи с гражданами в форме онлайновых консультаций, которые стимулируют дискуссии среди граждан, и демонстрируют в режиме реального времени агрегированный анализ коллективного мнения в разрезе тем, предложенных самими гражданами в процессе дискуссии.

Такой подход к реализации общественных консультаций позволит преодолеть вероятное отсутствие интереса к участию в них на условиях власти за счет реализации возможностей формирования повестки дискуссии самими участниками.

В докладе представлены результаты первого этапа проектирования онлайн-площадки для сайта Общественной палаты Санкт-Петербурга, а также план программы социальной рекламы и продвижения данного ресурса среди жителей Санкт-Петербурга.

Скатин А.В.
Россия, Санкт-Петербург, ООО «Консист»

ПЕРИОДЫ РАЗВИТИЯ АВТОМАТИЗАЦИИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Потребность органов государственной власти в автоматизации в настоящее время очевидна и продиктована задачами повышения эффективности и открытости работы органов государственной власти, что еще несколько лет назад рассматривалось как упрощение работы государственных служащих.

Целью данной работы является определение наиболее выделяющихся периодов автоматизации органов государственной власти, а также влияние современного состояния автоматизации органов государственной власти (ОГВ) на будущий период.

Проекты по автоматизации, для органов государственной власти, преимущественно регламентированы законодательной базой, как в части инициации, исполнения так и в содержательной части самого проекта. При этом можно проследить некоторые периоды автоматизации ОГВ, которые достаточно четко разделены, и обусловлены общим развитием отрасли информационных технологий и необходимостью выработки соответствующих законов.

Таким образом развитие ИТ отрасли и вырабатываемая законодательная база определяет основную функцию автоматизации ОГВ как обеспечивающую функцию.

Основная задача работы – это выделение различных периодов автоматизации органов государственной власти с учетом процессов развития ИТ отрасли.

Под автоматизацией в данной работе понимается разработка программно-аппаратных решений, интерфейсов взаимодействия различных участников, которые следуют за изменениями регионального или федерального законодательства.

Изначальный период современного развития автоматизации предлагал удобство выполнения или минимизацию выполнения рутинных операций вручную, назовем этот период «локальных АРМов» (АРМ – автоматизированное рабочее место). Во время периода «локальных АРМов» развивалась автоматизация локальных рабочих мест, что ускоряло работу определенных государственных служащих.

Следующий период был наиболее продолжительный и заключался в информационном обмене между различными органами государственной власти между собой, назовем этот период, периодом «Общей информации». Также этот период, в данной работе, обозначен как наиболее существенный для изменения законодательной базы. В силу того, что выделенный ОГВ всегда выполняет выделенную функцию и является первоисточником некоторой информации, но в данный период информация становиться общей для всех ОГВ и начинается использование механизмов общего хранения информации, что влечет существенную доработку законодательной базы. Во время периода «Общей информации» развивалась автоматизация механизмов информационного обмена, что ускоряло сквозные процессы между многими ОГВ регионального и федерального уровня. В данный период появляются характерные информационные системы, которые выполняют объединяющую функцию, такие как Государственная информационная система о государственных и муниципальных платежах и Система межведомственного электронного взаимодействия.

Третий период, который является текущим, помогает выполнять основную функцию ОГВ, которая направлена на гражданина, назовем этот период, как «Обеспечительный» период. В данный период изменение законодательства касается в большей степени регионального законодательства в силу специфики каждого в отдельности региона. На данном периоде появляется и развивается такие системы как Автоматизированные информационные системы многофункциональных центров.

Первый и второй периоды развития выглядят достаточно понятными и соответствуют периодам развития отрасли информационных технологий в целом. Третий период уже показывает, что автоматизация ОГВ наводится в зрелом состоянии.

Рассматривая автоматизацию ОГВ как систему, делаем предположение о следующем периоде развития, в основе которого будет лежать обратная связь, т.е. влияние гражданина на механизм взаимодействия с ОГВ, назовем этот период как «Самосовершенствующийся». Отметим, что в данном случае предположение не касается таких механизмов как опрос удовлетворенности взаимодействия граждан с ОГВ и т.п., а касается механизмов совершенствования автоматизации ОГВ как системы.

Заключение. Автоматизация органов государственный власти крайне важный механизм взаимодействия граждан и государственной власти. При этом такие аспекты как безопасность и доступность должны соблюдаться на любом периоде развития автоматизации. Предполагаемый будущий период автоматизации ОГВ требует проработки и осмысления. В частности необходимо определить базовые характеристики и ценности «Самосовершенствующегося» периода.

Чугунов А.В.
Россия, Санкт-Петербург, Университет ИТМО

РАЗВИТИЕ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ: ПО МАТЕРИАЛАМ СИСТЕМНОГО ПРОЕКТА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Важным документом, представляющим позицию российского правительства относительно развития технологий электронного правительства, является «Системный проект электронного правительства Российской Федерации» с горизонтом планирования до 2020 года. Этот документ еще не имеет официального статуса, но отражает позицию Минкомсвязи как ведомства, ответственного за эти задачи. Основанием разработки Системного проекта является поручение Президента Российской Федерации от 25 марта 2013 года № Пр-646.

В документе обозначено, что анализ предыдущего этапа развития электронного правительства показал целесообразность смены парадигмы его построения – перестройки на принципах клиенто-ориентированности, ориентации на формирование комплексной цифровой среды жизнедеятельности граждан и организаций с обеспечением постоянного роста качества электронных государственных и муниципальных услуг, оптимизации взаимодействия органов государственной власти (ОГВ) и местного самоуправления (ОМСУ) и вовлечения граждан в процессы управления.

Разработчики Системного проекта анализируют снижение позиции России в рейтинге ООН 2016 года и в качестве мер исправления ситуации предлагают реализовывать современные тенденции, связанные с внедрением технологий нового поколения, в том числе учитываемых в критериях ООН:

– реализация подхода «правительство как единое целое» (единая доверенная среда, единый дизайн и навигация электронных каналов доступа к услугам и официальных сайтов, в том числе в рамках информирования о деятельности органов государственной власти и местного

самоуправления, интеграция информационных систем в рамках предоставления электронных услуг и др.);

– расширение перечня услуг, предоставляемых полностью в электронном виде, включая возможность осуществить все необходимые платежи, - этот параметр имеет традиционно большое значение в методологии ООН;

– ориентация на пользователя и сокращение разрыва в возможностях использования электронного правительства, в частности, за счет предоставления эффективных специализированных электронных сервисов для различных социальных категорий населения;

– реализация полного набора инструментов электронного участия граждан в государственном управлении (включая информирование, экспертное консультирование, учет мнений при принятии решений) посредством внедрения и развития соответствующих электронных сервисов в инфраструктуре электронного правительства.

В документе впервые обозначена роль общественных организаций, как важного сектора, без которого невозможно достичь эффективного электронного участия граждан в государственном управлении. В Системный проект включены разделы «Развитие каналов взаимодействия гражданина с государством» и «Гражданское общество».

В частности подчеркивается в качестве актуальной задачи «учет и выделение новых и уточненных категорий пользователей электронного правительства для более индивидуального и проактивного удовлетворения запросов целевых сегментов аудитории». При этом констатируется, что некоммерческие организации в настоящее время взаимодействуют с органами власти по формату коммерческих структур, однако выделение некоммерческих (общественных) организаций в отдельную категорию пользователей связано со спецификой функционирования данного сектора (нацеленность на участие в принятии и контроле решений органов власти, потребность в инструментах самоорганизации и совместных действий). При этом, для организации совместной деятельности с некоммерческими организациями, помимо формирования отдельного набора услуг электронного правительства, требуется создание специальных инструментов, таких как сервисы площадок совместных действий или сервисы социальных сетей.

Важность компонента электронного участия обозначена в декларируемой цели, и выделана в качестве одной из трех основных задач реализации электронного правительства.

– обеспечение предоставления высококачественных государственных и муниципальных услуг (функций);

– снижение издержек реализации функций и осуществления полномочий ОГВ и ОМСУ, обеспечение принятия управленческих решений преимущественно в режиме реального времени;

– обеспечение возможности использования систем и сервисов электронного правительства для поддержки деятельности гражданского общества и бизнеса, в том числе их вовлечение в процессы государственного и муниципального управления.

В докладе представлены результаты анализа основных положений Системного проекта в контексте задач развития нормативной правовой базы и методического потенциала процессов региональной информатизации.

Шубинский М.И.
Россия, Санкт-Петербург, Университет ИТМО

СОЗДАНИЕ МЕЖРЕГИОНАЛЬНОГО ПИЛОТНОГО РЕСУРСНОГО ЦЕНТРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СЕВЕРО-ЗАПАДЕ РОССИИ

Один из самых важных вопросов, стоящих сейчас перед любым государственным учреждением с точки зрения применения информационных технологий, – это вопрос информационной безопасности. Однако особенно остро этот вопрос стоит перед учреждениями образования.

Риски, связанные с использованием сети Интернет, не ограничиваются опасностью заражения вирусами или хакерскими атаками. Проблема кибербезопасности (информационной безопасности), защиты детей от информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, особенно актуализирована в настоящее время. Проблемы, возникающие в связи с кибератаками и киберпреступностью, имеют далеко идущие последствия и должны решаться путем согласованной киберстратегии.

Образовательное учреждение должно выполнять все требования федерального законодательства по защите информации, например 152–ФЗ «О персональных данных» и 149-ФЗ «Об информации, информационных технологиях и о защите информации». Однако, например, сотрудники школ (учителя, инженеры) не имеют должной квалификации в вопросах защиты информации.

Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, подготовленные Министерством образования и науки Российской Федерации в 2014 году, указывают,

что в соответствии с Федеральным законом № 436-ФЗ (часть 1 статьи 14) должны проводиться организационно-административные мероприятия, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию. В том числе, мероприятия должны осуществляться по направлению «Повышение квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет»».

Создание пилотного учебно-методического ресурсного центра по направлению информационная безопасность позволит не только аккумулировать новейшие информационно-технологические и научно-методические ресурсы, предназначенные для повышения квалификации по направлению информационная безопасность, но и обеспечить условия устойчивой интеграции подобных межрегиональных центров в национальную систему образования России.

В рамках пилотного учебно-методического ресурсного центра можно будет произвести объединение технических, технологических и кадровых ресурсов для реализации Проекта, разработать новые и развить имеющиеся подходы, технологии и методики дополнительного профессионального образования, в том числе, с использованием технологий дистанционного обучения, соответствующих международным стандартам. Будут сформированы материально-техническая и нормативная базы, необходимые для реализации проекта.

Повышение качества общего образования за счет повышения квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет». Для реализации Проекта на первом этапе будет создан учебно-методический ресурсный центр по направлению информационная безопасность, с дальнейшим тиражированием опыта и результатов для увеличения зоны охвата регионов РФ. Созданный центр должен быть оснащен необходимым программно-аппаратным обеспечением, и аккумулировать в себе научно-методические и информационно-технологические образовательные ресурсы по направлению информационная безопасность.

В настоящее время в регионах РФ нет ни положительного опыта адаптации курсов повышения квалификации по вопросам информационной безопасности для нужд образовательных организаций, ни опыта повышения квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет». Для создания подобных положительных практик, объединяемых термином кибербезопасность, предлагается создать пилотный межрегиональный учебно-методический ресурсный центр, который бы занялся адаптацией существующих программ, апробированием их на практике и внедрением этих программ в ряде регионов.

В дальнейшем практику создания подобных ресурсных центров можно будет распространить и на остальные Федеральные округа.

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ

Балакирев Н.Е.
Россия, г. Москва, Московский авиационный институт (национальный исследовательский университет)

ПОТЕНЦИАЛЬНАЯ СУЩНОСТЬ ПЕРЕДАВАЕМОЙ И ВОСПРИНИМАЕМОЙ ИНФОРМАЦИИ

Фундаментальное свойство окружающего мира повторять свою неповторимость. Свою неповторимость любой физический объект отражает в виде информационного поля объекта, опирающегося при информировании о себе на физические поля, подвергаемые изменению при существовании объектов. Воздушную среду можно рассматривать тоже как некоторое поле, в котором молекулы воздуха при изменении давления передают свое «возмущение» соседним молекулам. Поле отражает единство и сплоченность, возникающие при изменениях извне. А в такой среде, пожалуй, единственным поставщиком осмысливаемой и распознаваемой информации для живущих являются волны, в самой природе которых заложена повторяемость. Волны, повторяясь в своей первозданности, омывают распознаваемый объект и, отражаясь от него, несут информацию о структуре и содержании объекта. Повторяемость при восприятии объектов гарант стабильности и объективности информации об объекте в пределах промежутка времени, определяемого скоростью его изменчивости. Но, она ведет и к избыточности и, если бы в отражении, фиксируемом живыми существами, хранилась вся получаемая информация, то не хватило бы никакой памяти для её хранения. «Борьба» с таким «злом» заключается в сжатии получаемой информации, преобразовании её в образ или игнорирование информации, забывание (затирание) такого образа. Отсюда понятно, что образ - это сжатая информация в виде некоторой структуры относительно оригинала. Но образ это не полная копия объекта, запечатленная принимающей стороной один в один, а некоторая модель, состоящая из достаточного набора примитивов, позволяющий отразить определенную глубину индивидуальности такого объекта.

Опираясь на физические методы передачи информации мы, так или иначе, сталкиваемся с повторяемостью, так как она носит аналогичный характер при обработке информации. При обмене информации в среде Интернет мы, чаще всего, базируемся на передаче смыслов в виде понятий, связки понятий. В основе большинства передач лежит передача образа буквы, оформляемой в компьютерном представлении в виде кодов, а на физическом уровне в виде передачи волн разных частоты или длины.

Фактически, при передаче и приеме (распознавании) информации наблюдается повторяемость в рамках любого выбранного алфавита. В основе кодирования такого алфавита лежит байт. Любое равномерное кодирование ведет к избыточности и это является основой для сжатия информации. Основной смысл сжатия, наиболее часто используемого при хранении и передаче информации, заключается в замене алфавита записи, в котором условная буква (новый образ) имеет переменную длину кода буквы по отношению к первоначальному равномерному коду. При этом часто используемые символы кодируются меньшим количеством бит, по отношению к редко используемым символам.

Физический уровень передачи звука в первую очередь использует определенный уровень (количество отсчетов) дискретизации, сохраняющий содержание, при котором информационно фиксируются амплитуды не всех точек волны, а только некоторые её представители при их равномерном распределении во времени. Более того, интуитивно понимая через эксперимент, что такое же прореживание возможно и при отражении значений амплитуд, переходят на логарифмический способ преобразования амплитуды в код, умещающийся значение амплитуды до размера байта, двойного байта или 20-разрядного кода.

Возможны ли другие способы или шаги в уплотнении информации? Безусловно, да! Основой такого утверждения является повторяемость, как волн, так и информационных конструкций, формируемых из волн, которые несут звуковую информацию. Использование логико-лингвистического подхода к структуризации волн, позволило практически сразу обеспечить сжатие информации по отношению к существующему способу цифрового представления звука. Введение и учет разных уровней представления информации открывает возможность поэтапного перехода на все более плотный (характеризуемый уменьшением объема памяти для хранения) способ записи звука, вплоть до перехода на фонемный технический алфавит. Полученные результаты уплотнения звука wav файла от 5 до 24 раз, подтвердили правильность теоретических и программных решений.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИНТЕРНЕТ ВЕЩЕЙ И ГИБРИДНЫЙ ИНТЕЛЛЕКТ

Как только в конце 40-вых годов прошлого века появилась электронная вычислительная машина, компьютер, так сразу же родилась аналогия между окружающим нас миром и компьютером, и эта аналогия продолжает развиваться и привлекаться для объяснения мироустройства (работы К. Цузе, Э. Фредкина, С. Ллойда и др.). Появление интернета вещей активизировало эти работы (М.Б.Игнатьев «Мир как модель внутри мирового суперкомпьютера»/ Доклад на семинаре Научного совета РАН по методологии искусственного интеллекта в Москве 30 июня 2016 г.).

Интернет вещей предполагает наличие связи с различными предметами, вещами, объектами. Следует заметить что и до этого связь с различными объектами поддерживалась людьми с помощью зрения, слуха и механического взаимодействия, но интернет вещей предполагает установление новой дополнительной связи с помощью различных технических средств, что позволит вещам взаимодействовать на новом уровне не только с людьми, но и вещам между собой. Далее, каждый из объектов описывается с помощью лингвистических, математических и компьютерных моделей. Например, солнечная система является специализированным вычислительным устройством для решения задачи многих тел. В итоге складывается следующая картина.

Во-первых, компьютеры – системы со структурированной неопределенностью, у них имеется память, которая может быть пустой или заполненной различными данными и программами. Доказано, что универсальные цифровые вычислительные машины могут решать самые разные задачи.

Во-вторых, описание мироустройства на естественном языке, который является универсальной знаковой системой, с помощью лингво-комбинаторного моделирования, превращается в систему уравнений с произвольными коэффициентами, которые и есть структурированная неопределенность. На использовании естественного языка основан и краудсортинг – выявление мнений умной толпы.

В-третьих, архитектура компьютеров непрерывно развивается – эволюционируют элементная база, уровень знаний компьютера, развиваются операционная среда и интерфейсы общения, системы ввода-вывода информации, системы контроля, диагностики и коррекции, системы передачи информации и энергии. Мир заполнен осцилляторами различных типов – это и атомы и молекулы, это и солнечная система и галактики , и все эти осцилляторы включены в общую моделирующую вычислительную систему.

В-четвертых, компьютеры являются вместилищем различных виртуальных миров, которые отделены друг от друга системами защиты информации. Наш мир – это виртуальная ячейка в мировом суперкомпьютере, который является неоднородной распределенной структурой, везде проникающей, а гигантский аналог 3D принтера может печатать астероиды, планеты и звезды.

В-пятых, компьютеры и сети являются основой самоорганизации социума.

Складывается сетевой гибридный интеллект на фоне развития интернета вещей на основе первобытного мышления. Наш современный опыт в своей совокупности составляется из относительно небольшого числа данных и бесконечного числа индукций. Опыт первобытного мышления, напротив, содержит индукции лишь в очень малой пропорции, но зато включает в себя много непосредственных данных, которым мы отказываем в объективной ценности, хотя они, на взгляд первобытного человека, тоже реальны и даже более реальны, чем данные внешних чувств.

Все это позволяет выдвинуть гипотезу о том, что компьютер можно рассматривать как базовую модель самоорганизации Вселенной.

При таком подходе становится понятным, почему нам до сих пор не удалось установить связь с инопланетянами. Ведь если наш мир не более чем модель внутри мирового суперкомпьютера, то для того, чтобы установить такую связь необходимо изучить структуру мирового суперкомпьютера, его аппаратного и программного обеспечения, изучить систему защиты между мирами, и вот тогда, может быть, удастся установить связь с обитателями других миров. Это колоссальная фундаментальная задача для современной науки (Kardashev N.S. “Transmission of Information by Extraterrestial Civilization”\\ Soviet Astronomy , vol.8, No 2, 1964; M.Ignatyev “ Galactic evolution simulation on basement of the linguo-combinatorial approach. Proceedings of the 29th GA IAUS317, 2015, Honolulu).

Ильина О.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МЕТОДОЛОГИЯ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ И СЕРВИСОВ

Термин «аудит» (audit) означает процедуру независимой проверки и оценки учётных и отчётных данных о деятельности организаций, различных систем, процессов, проектов или продуктов, которая выполняется строго в соответствии с законодательством. Аудит можно рассматривать и как разновидность контрольных, ревизионных или инспекционных процедур, конечной целью которого является повышение эффективности деятельности организаций.

Федеральный закон РФ № 403 от 1 декабря 2014 г. об аудиторской деятельности (аудиторских услугах по проведению аудита, оказанию сопутствующих аудиту услуг ввел основные понятия, определил требования к аудиторским организациям, индивидуальным аудиторам. В частности, в законе дается указание на необходимость соблюдения стандартов аудита, порядка проведения аудиторских проверок, наличие кодекса профессиональной этики для аудиторов.

Сегодня аудиторская деятельность существенно расширяет сферу применения, появились такие направления аудита, как: «операционный», «технический (промышленный)», «экологический», «качества» и т.д. В условиях информатизации систем управления возникает вопрос об аудите самих информационных систем (ИС) и информационных технологий (ИТ), а также информационных услуг/сервисов – ИТ-аудите. ИС включены в контур управления, они обеспечивают информационную и технологическую поддержку бизнес-процессов, учета, контроля и анализа деятельности организации, гарантируют определенный уровень информационной безопасности, но вносят также определенные риски в управленческий процесс, влияют на качество информацию. Во многих организациях ИТ-аудит является обязательной и систематической процедурой, выполняемой как самостоятельно (внутренний ИТ-аудит), так и с привлечением сторонних организаций (внешний ИТ-аудит).

Проведении ИТ-аудита предполагает следующие действия:

- Принятие решение о проведении ИТ-аудита.
- Выбор объектов, цели и задач ИТ-аудита, установление сроков, бюджета, формы ИТ-аудита: внутренний (силами ИТ-подразделения) или внешний (привлечение сторонней организации и экспертов).
- Обеспечение условий проведения ИТ-аудита, включая:
  - формирование команды аудиторов, назначение руководителя ИТ-аудита;
  - установление обязательных для соблюдения стандартов, норм и правил проведения ИТ-аудита, согласование аудиторского заключения по форме и содержанию;
  - разработка календарного план-графика ИТ-аудита;
  - разработка технологических инструкции по выполнению аудиторских проверок;
  - инструктаж лиц, вовлеченных в процесс ИТ-аудита.
- Формирование информационной среды ИТ-аудита.
- Управление ходом работ ИТ-аудита.
- Подготовка и защита аудиторского заключения.

ИТ-аудит следует рассматривать как проект, к которому применимы методы проектного управления, требующего специфических знаний (компетенций), ориентированного на лучшие практики аудиторских работ.

Цели и задачи ИТ-аудита связаны с проверкой состояния классов объектов, которые составляют информационную основу для процедур ИТ-аудита:

- «Требования бизнеса к ИС»
- «Архитектура ИС, архитектурные модели данных, приложений и ИТ-инфраструктуры».
- «ИТ-активы».
- «ИТ-процессы»
- «Персонал»
- «Документация ИС и ИТ-услуги/сервисы».

Для объектов классов следует регламентировать набор специфических атрибутов, установить нормативные значения отдельных атрибутов, определить задачи, методы и инструменты аудиторских работ, а также определить набор рисков, негативно действующих на объекты. Фактические значение атрибутов классов объектов устанавливается в процессе выполнения аудиторской проверки.

Класс «Требования бизнеса к ИС», согласно ГОСТ 34.602-89, содержит сведения, представленные в техническом задании на разработку ИС (общесистемные требования, требования к составу функций и задач, видам обеспечения ИС, надежности и безопасности, а также производительности и экономической эффективности ИС и др.). Класс «Архитектура ИС» выражает архитектуру построения ИС и ее компонентов, ИТ-стратегии, принципы построения ИС. Архитектура ИС представляется в виде дескриптивных моделей ее компонентов, например, по стандарту TOGAF – это архитектурные модели приложений, данных и ИТ-инфраструктуры ИС. Аудит архитектурных моделей ИС направлен на проверку синтаксической правильности конструкций архитектурных моделей, их точность и адекватность фактическому состоянию ИС. Общая оценка архитектуры ИС должна отражать актуальность, зрелость и возможность ее совершенствования и развития.

Класс «ИТ-активы» объединяет объекты, описывающие:

- информационные ресурсы ИС (системы документов, классификаторы и кодификаторы технико-экономической и социальной информации, базы данных, хранилища информации, веб-сайты и др.);

– программные ресурсы ИС (программная платформа ИС, прочие системные программы, прикладные программы, сервисы приложений, инструментальные средства разработки программных продуктов);

– технические ресурсы ИС (аппаратная платформа вычислительной системы, компьютерные сети, периферийное оборудование, средства оргтехники и т.п.).

В ходе ИТ-аудита выполняется инвентарная проверка наличия (сохранности) и характеристик ИТ-активов, правовых основ владения и использования ИТ-активов (лицензий, договоров), их необходимости и достаточности для эффективного функционирования ИС.

Класс «ИТ-процессы» объединяет категории процессов:

– управленческие – обеспечивают разработку стратегий ИТ, их соответствие требованиям бизнеса, повышение эффективности ИС и бизнеса;

– технологические – обеспечивают обработку информации согласно заявленным функциям системы управления организацией;

– обслуживающие – обеспечивают поддержку ИС в работоспособном состоянии, информационную безопасность, работу пользователей ИС и др.

ИТ-процессы должны быть регламентированы по применяемым стандартам, составу операций, исполнителям, информационному и технологическому сопровождению. Аудит ИТ-процессов призван выполнить проверку производительности, оценить зрелость процессов и эффективность использования ресурсов ИС в ИТ-процессах.

Класс «Персонал» включает объекты, характеризующие ИТ-персонал и пользователей ИС. Сопровождение ИС осуществляется службой ИТ или внешней аутсорсинговой организации. Аудит нацелен на проверку штатного расписания, должностных инструкций, отражающих квалификационные требования к персоналу, технологических инструкций выполнения работ по сопровождению ИС. Для конечных пользователей ИС устанавливается техминимум, который обеспечивает допуск к работе в ИС, доступ и конфигурация автоматизированного рабочего места, правила.

Класс «Документация ИС и ИТ-услуги/сервисы» описывает формы документов, схемы документооборота в ИС.

Аудиторское заключение для ИС и ИТ должно содержать ряд аргументированных выводов и заключений, полученных в результате анализа данных об объектах ИТ-аудита, а именно:

1. Оценка нормативной базы ИС и ИТ. Рекомендации по использованию COBIT, ITIL отечественных и международных стандартов информационных технологий.

2. Рекомендации в части методологии управления и методов менеджмента ИС и ИТ.

3. Рекомендации по архитектуре ИС в части отдельных архитектурных моделей: актуализация моделей, реинжиниринг, переход к новой архитектуре и т.п.

4. Оценка состояния ИТ-активов ИС различных категорий, общие рекомендации по их развитию.

5. Оценка и рекомендации для отдельных ИТ-процессов: требования роста производительности, уровня зрелости, документирования, внесения изменений в ИТ-процессы, реинжиниринга ИТ-процессов и т.п.

6. Оценка эффективности использования трудовых, материальных, вычислительных и информационных ресурсов для функционирования ИС, влияния ИС и ИТ на эффективность бизнеса.

7. Оценка работы ИТ-подразделения и конечных пользователей, рекомендации по численности и компетентности, системам подготовки и обучению персонала для работы в ИС.

8. Оценка перспектив развитию ИС и ИТ.

Для внутреннего ИТ-аудита целесообразно использовать информационные системы классов ITAM – Information Technology Asset Management, управление активами и ITIL - Information Technology Infrastructure Library, сервисы для поддержки функционирования ИС и

Касаткин В.В., Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Имитационное моделирование (ИМ) является не только эффективным инструментом исследования функционирования информационно-управляющих систем (ИУС) на этапе их проектирования: в современных системах управления сложными объектами на основе моделирования, реализуемого непосредственно в контуре управления, решаются задачи прогнозирования и оптимизации для последующего принятия решений по управлению объектом и выработки управляющих воздействий. Создание ИУС требует наличия большого объема информации как о самом объекте, так и о его входных и выходных переменных. Эта информация необходима для построения адекватной модели, на основе которой может быть эффективно

реализован процесс управления. При этом используются два вида информации, необходимой для построения и совершенствования системы управления: априорная и текущая.

Априорная информация об объекте управления, его входных и выходных переменных, внутренних состояниях необходима для построения модели, в результате исследования которой создается система управления объектом: выбирается структура, алгоритмы и параметры системы управления, критерий функционирования. Обычно для вновь проектируемых сложных объектов отсутствует готовая модель, необходимая для создания системы управления, и задача управления решается в условиях недостаточной или вовсе отсутствующей априорной информации об объекте. Речь идет об отсутствии формализованного описания информационной («управленческой») модели объекта управления, устанавливающей взаимосвязь между выходными и входными переменными.

Необходимость получения текущей информации, в случае, когда система управления создана и функционирует, может быть обусловлена двумя факторами. Во-первых, – это потребность в непрерывном совершенствовании ИУС, во-вторых, – необходимость уточнения поведения системы, ее состояния и возникающих в ней ситуаций с целью компенсации изменений характеристик системы как объекта управления. Процессы, с которыми связана текущая информация в первом случае, являются достаточно медленными, для управления которыми используется подсистема эволюционного управления. Процессы второго типа являются более быстрыми, и для управления ими необходима подсистема оперативного управления, функционирующая в реальном масштабе времени.

Важнейшей задачей современной теории и практики управления является формализация закономерностей функционирования сложного объекта, т.е. построение и исследование модели объекта управления, на основе которой определяются структура, алгоритмы и параметры системы управления, выбираются аппаратно-программные средства их реализации. Построение информационной модели методами идентификации должно быть направлено на ликвидацию этого разрыва и разработку методов оперативного получения моделей сложных объектов управления с использование ЭВМ.

Невозможность применения единой универсальной ИМ обусловлена тем, что, с одной стороны, при построении указанных моделей ставятся различные цели, а с другой стороны, модели описывают процессы, протекающие в различных масштабах времени, причем степень полноты модели, ее соответствие реальному объекту зависят от задач, для решения которых эта модель предназначена. Модели первого типа имеют в основном гносеологический характер, от них требуется тесная связь с методами исследования конкретной области знаний, для которой они строятся. Модели такого типа являются достаточно «инерционными», так как отражают эволюцию в конкретной области знаний (эволюционные модели). Модели второго типа носят информационный характер и должны соответствовать конкретным целям, связанным с принятием решений по управлению объектом, который они описывают (десиженсные модели). Несмотря на относительную условность деления моделей на гносеологические (эволюционные) и информационные (десиженсные), их использование удобно для классификации задач и отражения целей моделирования.

В информационных ИМ, используемых непосредственно для принятия решений в системах управления сложными объектами, требование оперативности является одним из основных. Это обусловлено тем, что при каждом воздействии на объект управления в ИМ должны учитываться действительные изменения, произошедшие в объекте, а также внешние возмущения, на основе которых осуществляется управление. Указанное требование, связанное с необходимостью обеспечения работы ИМ в реальном масштабе времени, часто приводит к отказу от более сложных и точных моделей и разработке робастных алгоритмов построения моделей, использование которых в ИУС приводит к достижению поставленной цели.

Морозов С.А
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

РЕАЛИЗАЦИЯ VFS В UNIX ПОДОБНЫХ СИСТЕМАХ

VFS (virtual file system – виртуальная файловая система) – система, которая представляет собой уровень абстракции, находящийся поверх реальных файловых систем и обеспечивающий всем приложениям пользовательского пространства (user space) единообразный доступ к ресурсам, не зависимо от реальной конкретной файловой системы. VFS может быть использована, например, для доступа к локальным или сетевым устройствам хранения информации прозрачно для клиента.

В UNIX, традиционно, используется модель Node Graph (граф состоящий из узлов). Эта модель представляет файловую система как граф, узлы которого могут выступать в роли файла, директории или другую точку монтирования.

VFS описывает файлы системы с помощью суперблоков и inode-структур, во многом таким же образом, как ext2 использует суперблоки и дескрипторы. Как и в ext2, VFS inode структуры описывают файлы, директории и топологию системы в общем.

VFS в Linux используют единый кэш буфер (cache buffer) для всех использующихся файловых систем и физических устройств в система для обеспечения оптимального доступа к данным. Этот буфер независим от реальных файловых систем и интегрирован в механизмы, которые ядро Linux использует для выделения, чтения и записи суперблоков для любой конкретной файловой системы.

Мотиенко А.И., Салухов В.И., Солдатенко Т.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

УПРАВЛЕНИЕ ГЕОЭКОЛОГИЧЕСКИМ РЕЗЕРВОМ ИНФРАСТРУКТУРЫ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА

В последние годы проводятся активные исследования по созданию системы обеспечения защиты природно-техногенных систем от негативного воздействия строительной отрасли и жилищно-коммунального хозяйства. Основной целью указанной системы является минимизация негативного воздействия на окружающую среду от функционирования объектов указанных отраслей.

Жилищно-коммунальное хозяйство (ЖКХ) является крупнейшей сферой экономики страны и играет важнейшую роль в обеспечении нормальных условий проживания и существования граждан. Вместе с тем, деятельность ЖКХ относится к одному из наиболее мощных факторов негативного воздействия на окружающую среду по преобразованию природно-техногенных систем. Одной из основных причин указанного негативного воздействия объектов инфраструктуры ЖКХ является недостаточно эффективное управление ее геоэкологическим резервом.

Под указанным резервом в настоящей работе понимается совокупность мер, приводящих к снижению негативного воздействия ЖКХ на окружающую среду. Под управлением геоэкологическим резервом в статье понимается выбор предупредительной меры для объекта инфраструктуры (ОИИ) ЖКХ, при которой обеспечивается необходимый уровень данного резерва.

В статье рассмотрен подход к математическому моделированию социально-экономической системы инфраструктуры ЖКХ по обеспечению требуемого уровня геоэкологического резерва в виде заданной величины вероятности недостижения техническим состоянием ОИИ предельного состояния и обоснованию неотложных мер, соответствующих конкретной ситуации.

В статье указанная вероятность рассматривается как целевая функция процедуры выбора оптимальной по критерию минимума риска аварии ОИИ меры по обеспечению геоэкологического резерва. Ограничениями выступают допустимые уровни затрат ресурсов на реализацию соответствующих мероприятий. Приводится расчетный пример.

Охтилев М.Ю., Потрясаев С.А., Соколов Б.В
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МЕТОДОЛОГИЯ И ТЕХНОЛОГИЯ КОМПЛЕКСНОГО МОДЕЛИРОВАНИЯ СЛОЖНЫХ ТЕХНИЧЕСКИХ ОБЪЕКТОВ

В настоящее время для повышения степени оперативности и достоверности прогнозов развития существующих и проектируемых сложных технических объектов (СТО), а также проактивного управления ими в таких наукоемких отраслях экономики как судостроение, аэрокосмическая отрасль, топливно-энергетические, военно-технический комплексы и т.п., требуется проведение упреждающего многовариантного моделирования различных сценариев их функционирования в динамически изменяющейся обстановке. Проактивное управление в отличие от традиционно используемого реактивного управления СТО, ориентированного на оперативное реагирование на складывающуюся ситуацию и компенсацию непредвиденных возмущений за счет обратной связи, предполагает предотвращение возникновения инцидентов путем создания в соответствующей системе мониторинга и управления принципиально новых упреждающих возможностей при формировании и реализации управляющих воздействий, основанных не на парировании следствий, а причин, вызывающих возможные нештатные, аварийные и кризисные ситуации в СТО. При этом на практике для описания таких ситуаций наиболее часто используются имитационные моделирование и соответствующие имитационные модели и эвристические алгоритмы. Однако, как показывает анализ, на современном этапе развития теории и технологий имитационного моделирования уже нельзя никак обойтись без рассмотрения вопросов его взаимодействия с другими теориями и технологиями моделирования в рамках интенсивно развивающейся методологии и технологии комплексного (системного) моделирования (КМ), которые базируются на полимодельном описании СТО, а также комбинированном использовании методов, алгоритмов и методик многокритериального анализа, синтеза и выбора наиболее предпочтительных управленческих решений, связанных с созданием, использованием и развитием СТО в различных условиях динамически изменяющейся внешней и внутренней обстановок. Идейная сторона КМ была заложена в начале XX века великим физиком Н. Бором при формулировке им принципа дополнительности. Основное достоинство КМ состоит в том, что за счет полимодельного (многомодельного) описания каждой конкретной исследуемой предметной области, где используются

СТО, и соответствующего согласования разнотипных моделей, методов и алгоритмов анализа и синтеза СТО на формализованном (глубинном) уровне их описания удается, во-первых, взаимно компенсировать недостатки и ограничения, присущие каждому частному классу моделей, методов и алгоритмов, и, во-вторых, получить синергетический эффект от их интегративного использования, выражающийся в формировании новых знаний о СТО и его поведении. В докладе представлен научно-методический аппарат (методологические основы, модели, методы, алгоритмы и технологию) комплексного моделирования процессов функционирования системы проактивного управления СТО, базирующийся на прикладной теории управления структурной динамикой СТО, которую авторы развивают вот уже более 25 лет. Практическая апробация результатов будет проиллюстрирована применительно к СТО, создаваемым в ракетно-космической отрасли промышленности РФ.

Рыжков С.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ ПЕРИМЕТРА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Задача прогнозирования вероятных нарушений безопасности, которые связанны с непосредственным обнаружением нарушения динамического периметра облачных вычислений в режиме реального времени обусловлена необходимостью создания и контроля периметра информационной безопасности в совокупности с соотношением цифрового и географического ландшафтов.

Важным условием для обеспечения информационной безопасности (далее ИБ) информационной системы, построенной с использованием технологий облачных вычислений, является определение потенциального места проведения атаки с целью её предотвращения, а наиболее перспективным направлением решения описанной проблемы являются геолокационные метки, так называемые геометки, технология, позволяющая гарантированно определять местоположение обрабатываемых данных.

Инструменты автоматического обнаружения позволяют сократить время обнаружения, а также снизить требования к уровню подготовки специалиста за счёт шаблонов инцидентов ИБ и профилей нарушителя, а также структуризации данных.

Системы информационной безопасности, использующие когнитивные технологии, оперируют неструктурированными массивами данных с помощью различных математических моделей когнитивного мышления эффективнее человека-оператора.

Даже высококвалифицированные специалисты не в состоянии контролировать большой поток данных от различных информационных процессов в реальном времени, постоянно поступающих сигналов от различных периферийных устройств инфраструктуры безопасности (BigData).

При построении периметра информационной системы с использованием нейросетей создаётся условная граница, соотносящая цифровой и географический ландшафты, а также предоставляющая возможность районирования.Граница, представляющая цифровой и географический ландшафты корректируется с помощью таблиц маршрутизации.

Согласно определённому шаблону информационной безопасности система, в режиме реального времени позволит оператору контролировать конфигурацию безопасности, с возможностью идентифицировать известные и новые угрозы безопасности за счет использования когнитивной системы прогнозирования и выявления нарушений информационной безопасности в динамических средах, позволит проводить самотипизацию поступающего массива данных.

Благодаря методам, которые моделируют когнитивные способности человеческого мозга, системы ИБ помогают оператору в прогнозировании и выявлении нарушений информационной безопасности. Сочетая возможности традиционного программного обеспечения, аппаратного оборудования и адаптивного модуля когнитивного анализа данных.

Предлагается использовать адаптивную нейро-нечеткую систему вывода ANFIS (Adaptive Network-based Fuzzy Inference System), которая реализует систему нечеткого вывода Сугено в виде пятислойной нейронной сети прямого распространения сигнала. Актуальность этой технологии – нечеткое моделирование, обусловленное тенденцией увеличения сложности математических моделей в системе реального времени.

Салухов В.И., Солдатенко В.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МОДЕЛЬ ИННОВАЦИИ ДЛЯ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ЭКСПЕРТИЗЫ ПРОЕКТА СЕТИ СВЯЗИ

В работе рассмотрен подход к оцениванию эффективности экспертизы проекта сетей связи на основе использования инновационных технологий. Инновация рассматривается как материализованный результат, полученный от вложения капитала при инновационной деятельности в новую технику или технологию, в новые формы организации производства труда, обслуживания,

управления и т.п. При этом исследуется применение процессно-утилитарного подхода в инновационной деятельности к оцениванию эффективности экспертизы проекта сетей связи.

Предложено рассматривать процесс проектирования сети связи как последовательность нескольких необходимых (обязательных) этапов преобразования некоторой исходной информации о предполагаемых свойствах сети. Сделан вывод о том, что при проведении соответствующих экспертных действий на более ранних этапах указанного цикла уровень качества проектной документации будет выше. Для количественного обоснования этого вывода предложен подход к построению инновационной технологии осуществления экспертизы проектной документации. Этот подход базируется на исследовании влияния обратной связи на точность преобразования информации, поступающей на начало соответствующего этапа преобразования при проектировании.

При построении модели инновационного подхода к проведению экспертизы проектной документации предложено использовать вероятностный подход. Он состоит в том, чтобы принимать во внимание случайный характер осуществления неправильных действий при анализе исходной для некоторого этапа преобразования информации. Исследованы наиболее распространенные способы осуществления экспертизы. Для каждого из них получены результаты моделирования в соответствии с предложенным подходом.

Анализ полученных результатов моделирования позволяет определить наиболее предпочтительный вариант экспертного оценивания проекта телекоммуникационной системы в зависимости от состава исходных данных об условиях проведения экспертизы проекта. Расчетные результаты показывают, что направление моделирования выбрано правильно и может быть применено для обоснования инновационных технологий экспертного оценивания проектной документации в сфере телекоммуникаций.

Свиньин С.Ф., Алексеев А.В., Попов А.И., Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный морской технический университет, Северный (Арктический) федеральный университет имени М.В. Ломоносова

ТЕОРИЯ ИНФОРМАЦИИ: ОТ ТЕОРЕМЫ УИТТЕКЕРА-КОТЕЛЬНИКОВА-ШЕННОНА К ТЕОРИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ

30 апреля 2016 года исполнилось 100 лет со дня рождения Клода Э́лвуда Ше́ннона.

В канун знаменательной даты в Санкт-Петербургском институте информатики и автоматизации Российской академии наук состоялось специальное заседание ученой общественности, посвященное этому событию. На юбилейном семинаре были заслушаны доклады о научной биографии основателя современной теории информации К.Шеннона, основных его заслугах в области теории связи и теории информации. Отмечено, что фундаментальная теорема отсчетов в теории информации не утратила своей актуальности и сегодня, имеет ряд вариантов современной трактовки.

Принцип финитности спектров по-прежнему является одним из определяющих граничные условия перехода к дискретным сигналам и их цифровой обработке, для исследования которых все большее применение находит целый спектр методов функционального анализа.

Энергетические пространства, сигналы с конечной энергией, функции с компактными носителями широко используются сегодня в арсенале исследовательских средств. Представление модели сигналов функциями времени конечной длительности, а также использование вейвлет-базисов и обобщенных алгоритмов быстрых спектральных преобразований позволяют сегодня решать самые сложные задачи тонкого спектрального, кепстрального анализа и других.

Участникам юбилейной встречи были представлены целый ряд современных методов исследования тонкой структуры сигналов, включая анализ биомедицинских сигналов большой длительности. Применение теории отсчетов при изучении двигательной деятельности органов желудочно-кишечного тракта человека, анализе результатов цифровой электро-гастро-энтерографии с различными диапазонами и полосами гармонического анализа позволяет сегодня результативно решать конкретные практические задачи диагностики заболеваний и прогнозирования их динамики.

Особое внимание участников юбилейной встречи было уделено анализу фундаментального значения теоремы отсчетов Уиттекера-Котельникова-Шеннона (теоремы УКШ), развитие которой, по мнению участников, насчитывает сегодня более пяти исторических этапов, включая:

– «математический период» выявления закономерности представления временных функций массивом выборочных значений, кардинальной функцией интерполяции (E.T.Whittaker);

– «телеграфный период» освоения выявленной закономерности в прикладных областях знаний и практической деятельности (H.Nyquist, В.А. Котельников);

– «связной период» обобщения закономерности и теоремы отсчетов для задач связи при наличии шума и перехода к информационной парадигме (К. Шеннон);

– «интерферренционный период» обобщения закономерности и теоремы отсчетов с учетом и контролем мощности помех наложения спектров (мимикрии частот, алайзинга и т.п.);

– «оптимизационный период»спектральной интерпретации процессов дискретизации и квантования с обобщением теоремы отсчетов на основе учета специфики, динамического диапазона и погрешностей преобразования полосовых финитных процессов с возможностью оптимального («двухстороннего») без избыточного выбора частоты дискретизации.

Анализ тенденций развития современной теории информации в условиях революционных изменений информационных технологий с терабитными возможностями вместе с тем указывает на необходимость концентрации усилий исследователей на вопросах её прикладной теории (профессор И.М. Коган), а также теории ценности информации (академик А.А. Харкевич), теории измерения её качества (квалиметрии) и полимодельного представления.

Это позволит, с одной стороны, усилить поиски путей и результативность минимизации избыточности обрабатываемых данных, как «вечной проблемы» теории информации. С другой стороны, станет возможным системно обоснованно и принципиально решать вопросы информационно-технического сопряжения психофизиологических возможностей операторов с возможностями современных информационно-управляющих систем при комплексной информационно-аналитической и интеллектуальной обработке данных, поступающих с мониторов эргатических комплексов и систем, а также - поддержке принятия управленческих решений. Это сегодня все более представляет проблему, требующую неотложного решения, в результате чего будет обеспечено информационно комфортное пространство управления все более сложными современными робототехническими системами.

Наконец, наряду с другими позитивными изменениями создание и интенсивное развитие теории управления информационным пространством позволит уже в ближайшей перспективе войти более подготовленными в полосу неминуемых широкомасштабных сетецентрических и информационных противоборств, что всегда оставалось и будет одной из ключевых национальных задач, а сегодня уже проявляется с особой силой в целом ряде направлений межгосударственных отношений.

Терехин Д.В., Климов А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

РОЛЬ И МЕСТО РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ ПРИ ОРГАНИЗАЦИИ КОЛЛЕКТИВНОЙ РАБОТЫ НА СРЕДСТВАХ АВТОМАТИЗАЦИИ

Децентрализация обработки данных находит в настоящее время все большее использование при организации коллективной работы. Подобный подход расширяет возможности совместного использования информации, одновременно повышая эффективность доступа к ней. Там распределенные базы данных(РБД) обеспечивают общедоступность данных для всех пользователей при этом обеспечивая их хранение именно в тех местах, где они чаще всего используются. Это так же повышает устойчивость информации к одновременной утрате вследствие технических сбоев в работе оборудования и позволяет решить проблему «информационных островов».

Распределенные системы баз данных имеют дополнительные преимущества перед традиционными централизованными системами баз данных. К сожалению, эта технология не лишена и некоторых недостатков.

Наряду с экономической выгодой использования преимуществами РБД являются: отражение структуры организации; модульность системы, разделяемостъ и локальная автономность; повышение доступности данных и надежности.

К недостаткам РБД наряду со сложностью их разработки и требованиям по уровню подготовки технического персонала так же относят повышение сложности, стоимости, проблемы в организации защиты информации и контроля за информацией, а так же отсутствие стандартов их использования.

Основной принцип РБД заключается в "прозрачности распределенности". С точки зрения пользователя информации распределенная БД не должна отличаться от локальной БД. Здесь имеется в виду пользователь, формулирующий запросы к базе данных и получающий результаты на своем экране (или принтере). Технология его работы не должна зависеть от того, в какой конкретной базе находятся нужные ему данные: в его локальной базе, в удаленной базе, все необходимые данные в одной и той же базе или в различных базах данных.

Таким образом создание корпоративных БД - деятельность, использующая многие методы классического проектирования, но требующая иной организации и многих дополнительных методов, а также новых, которые заменили бы некоторые из тех, что были разработаны 10 и более лет назад.

Классические методы проектирования БД должны продолжать использоваться, но только в тех в областях, где они действительно полезны. Методы проектирования, рассматриваемые в конкретных проектах корпоративных информационных систем и БД, и соответствующие инструменты должны проверяться на свои возможности обеспечивать свои функции в соответствии с требованиями проектирования.

Большой рост объемов БД будет сопровождаться ростом требований к их надежности. К средствам и методам проектирования БД вследствие постоянно осуществляемого процесса

перепроектирования БД будут непосредственно примыкать средства управления БД. Так, для обеспечения устойчивых к отказам данных необходимо владение средствами управления и синхронизации географически разнесенных теневых и резервных баз данных.

Хомоненко А.Д., Халил М.М., Андрук А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

АЛГОРИТМЫ РАСЧЕТА ОПЕРАТИВНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ПОМОЩЬЮ МОДЕЛЕЙ МНОГОКАНАЛЬНЫХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ С «ОХЛАЖДЕНИЕМ»

В докладе рассматриваются вопросы оценивания оперативности облачных вычислений, доступ к которым обеспечивается с помощью Веб-интерфейса. Названный интерфейс реализуется на основе приложений Java с помощью сервлетов и фильтров. При этом для оценки оперативности функционирования таких приложения предлагается использовать численный аппарат теории массового обслуживается. При этом рассматриваются алгоритмы исследования характеристик моделей многоканальных не Марковских систем массового обслуживания (СМО).

Эти модели позволяют оценить оперативность функционирования приложений с Java на основе веб-интерфейса с использованием фильтров. Обсуждаются результаты исследования вопросов, как фильтры влияют на общую производительность облачных сервисов, поскольку производительность является одним из ключевых факторов использования.

Алгоритм расчета оперативности функционирования приложений с Веб-интерфейсом основан на моделях многоканальных систем с "охлаждением" и использовании аппроксимирующих распределений фазового типа для марковизации не Марковских процессов. Получены переходные диаграммы и матрицы для микросостояний модели СМО приложения с веб-интерфейсом, а также схемы для вычисления стационарных распределений вероятностей числа запросов в системе и распределения времени ожидания.

Для изучения облачных систем с помощью предлагаемой модели СМО с "охлаждением" полезно использовать расширенное обозначения Кендалла вида A/S/C/N, которое по сравнению с оригинальным обозначением (A – входящий поток, S – обслуживание, n – число каналов) содержит символ C, обозначающий распределение времени охлаждения.

Моделирование проведено для системы массового обслуживания с "охлаждением" M/M/E2/n с пуассоновским входящим потоком (M), экспоненциальным распределением длительности обслуживания (M) и распределением Эрланга 2-го прядка длительности «охлаждения» E2. Оцениваются: среднее число заявок в системе - L, средняя длина очереди - Lq, среднее время ожидания в очереди - Wq, и среднее время пребывания в системе - W, при изменении частоты охлаждения.

Исследование демонстрирует влияние работы фильтров (моделируется с помощью «охлаждения») на производительность и показывает необходимость сбора данных и изучения параметров «охлаждения» модели, чтобы гарантировать, что возможности облачной системы подходят для существенно различных уровней и структуры спроса, которые могут иметь место в течение определенного периода времени.

Трофимов В.В., Трофимова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

КАТЕГОРИАЛЬНЫЙ АНАЛИЗ ТЕРМИНА «ИНФОРМАЦИЯ»

Наиболее часто под информацией понимают: сведения; сообщения о чем-либо, которыми обмениваются люди; сигналы; импульсы; образы, циркулирующие в технических (кибернетических) устройствах; количественную меру устранения неопределенности (энтропии); меру организации системы; отражение разнообразия в любых объектах и процессах неживой и живой природы; знание как связи между фактами.

Есть и другие определения информации, но все они зачастую несовместимы друг с другом, например, Информацией именуются: абстрактный концепт, физическое свойство, функция самоуправляемых систем. Информация может быть: объективной и субъективной, материальной и идеальной. Информация – это и вещь, и свойство, и отношение.

Для упорядочивания этих определений проведен категориальный анализ и рассмотрены различные содержания, вкладываемые в термин «информация», которые в свою очередь позволили предложить следующую классификацию подходов к выявлению смысла, вкладываемого в этот термин: 1. метрологический - описывающий возможные шкалы измерения различных характеристик термина (объемный, предлагающий метрику для измерения емкости для хранения информации; энтропийный, предназначен для описания требований, предъявляемых к скорости передачи данных по каналу; алгоритмический, определяющий требования к алгоритму преобразования входной информации в выходную; семантический, определяющий полезность информации, исходя из размер словаря пользователя; аксеологический, позволяющий оценивать информацию, исходя из её

полезности для пользователя; 2. материалистический, рассматривающий информацию как атрибут (неотъемлемую часть) материи и утверждающийся, что информация без материи существовать не может, или как функцию самоорганизующихся систем; 3. ведический, признающий первичным сознание по отношению к материи, и утверждающий таким образом, что сознание порождает материю. В этом случае знание (информация) порождается в результате взаимодействия атмы (спиритона) со сверхсознанием (абсолютом) и с материей.

Применение данных подходов позволяет корректно использовать термин «Информация» при описании и интерпретации результатов в одной конкретной предметной области и установить границы применимости данного термина и смыслы, вкладываемые в него.

Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНТЕЛЛЕКТУАЛИЗАЦИЯ МАШИННОЙ ИМИТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

В докладе обсуждаются два понятия: «имитация» и «интеллект», которые относятся, на первый взгляд, к разным предметным областям (ПрО).

Сформулируем основные требования, предъявляемые к имитационной модели (ИМ) процесса функционирования информационной системы (ИС).

1. Полнота ИМ должна предоставлять пользователю возможность получения необходимого набора оценок характеристик ИС с требуемой точностью и достоверностью.

2. Гибкость ИМ должна давать возможность воспроизведения различных ситуаций при варьировании структуры, алгоритмов и параметров ИС.

3. Длительность разработки и реализации ИМ большой ИС должна быть по возможности минимальной при учете ограничений на имеющиеся ресурсы.

4. Структура ИМ должна быть блочной, допускать возможность замены, добавления и исключения некоторых частей без переделки всей ИМ, т. е. архитектура ИМ должна быть открытой.

5. Информационное обеспечение должно предоставлять возможность эффективной работы ИМ с базой знаний (БЗ) ИС определенного класса.

6. Программные и технические средства должны обеспечивать эффективную (по быстродействию и памяти) машинную реализацию модели и удобное общение с ней пользователя, т. е. предполагается наличие дружественного интерфейса.

7. Должно быть реализовано проведение целенаправленных (планируемых) имитационных экспериментов с ИМ ИС с использованием аналитико-имитационного подхода при наличии ограниченных вычислительных ресурсов.

Теперь, если обратится к требованиям к разработке экспертной системы (ЭС) для ПрО ИС, то они на 90% пересекаются. Действительно, при разработке прототипа ЭС в настоящее время сложилась определенная технология проектирования ЭС, которая включает следующие шесть этапов: идентификация, концептуализация, формализация, выполнение, тестирование и опытная эксплуатация.

Этап идентификации связан, прежде всего, с осмыслением задач проектирования ИС, которые предстоит решить будущей ЭС, и формированием требований к ней. Результатом данного этапа является ответ на вопрос, что надо сделать и какие ресурсы необходимо задействовать (идентификация задачи, определение участников процесса проектирования и их роли, выявление ресурсов и целей).

На этапе концептуализации проводится содержательный анализ ПрО, выявляются используемые понятия ИС и их взаимосвязи, определяются методы решения задач. Этот этап завершается созданием модели ПрО, включающей основные концепты и отношения.

На этапе формализации все ключевые понятия и отношения выражаются на некотором формальном языке, который либо выбирается из числа уже существующих языков, либо создается заново. Другими словами, на данном этапе определяются состав средств и способы представления декларативных и процедурных знаний, осуществляется это представление и в итоге формируется описание решения задачи ЭС на предложенном (инженером по знаниям) формальном языке.

Цель этапа выполнения — создание одного или нескольких прототипов ЭС, решающих требуемые задачи разработки ИС. Разработка прототипа ЭС состоит в программировании его компонентов или выборе их из известных инструментальных средств и наполнении БЗ. Главное в создании прототипа заключается в том, чтобы этот прототип обеспечил проверку адекватности идей, методов и способов представления знаний решаемым задачам проектирования ИС.

В ходе этапа тестирования производится оценка выбранного способа представления знаний в ЭС в целом. Для этого инженер по знаниям подбирает примеры, обеспечивающие проверку всех возможностей разработанной ЭС. При этом различают следующие источники неудач в работе системы: тестовые примеры, ввод-вывод, правила вывода, управляющие стратегии.

На этапе опытной проверяется пригодность ЭС для конечного пользователя, т. е. проектировщика ИС. Пригодность ЭС для пользователя определяется в основном удобством работы с ней и ее полезностью.

Таким образом, ИМ и ЭС, создаваемые для целей проектирования целого класса ИС, сливаются воедино: 1) в ИМ с элементами интеллекта (работа со знаниями ПрО) или 2) в ЭС с элементами имитации (работа в динамике ПрО).

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

Авраменко В.С., Бобрешов-Шишов Д.И., Соловьев В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИДЕНТИФИКАЦИЯ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Согласно общедоступным статистическим данным большинство зарегистрированных компьютерных атак в инфокоммуникационных системах различного назначения связаны с внутренними нарушителями. Одной из проблемных задач, часто возникающих при обнаружении атаки, является идентификация личности и (или) компьютера нарушителя (как правило, нарушители используют «чужие» логины и компьютеры).

Обычно задача идентификации нарушителя решается администраторами практически вручную с помощью различных программных и технических средств по индивидуальным методикам, сформировавшихся на основе собственного опыта. Однако такой подход занимает длительное время, не всегда приводит к успеху.

Перспективным путем решения данной проблемы является автоматизация процесса идентификации нарушителя (или ЭВМ нарушителя) на основе объективных данных о его индивидуальных признаках. Наиболее достоверны и доступны для наблюдения признаки, наблюдаемые в сети. Современные средства наблюдения, контроля и анализа сетевого трафика позволяют выделить «пакеты» нарушителя, даже использующего различные способы маскировки. Изучение трафика нарушителя позволяет определить значительное количество идентификационных признаков. Такие признаки можно разделить на технические и личностные.

К техническим относятся такие признаки, на основе наблюдения и анализа которых возможно идентифицировать ЭВМ нарушителя. Примерами технических признаков могут служить: IP и MAC адреса атакующего компьютера, версия и язык операционной системы, параметры экрана и другие.

Под личностными подразумеваются такие признаки, на основе которых можно определить личность пользователя. Примерами личностных признаков являются следующие: язык программного интерфейса, используемый пользователем; применяемые для работы с сетевыми ресурсами программные средства (например, тип браузера, клиента электронной почты, мессенджера), количество попыток авторизации, обычное время входа компьютера в сеть, длительность сеанса работ и другие).

По одному признаку однозначно идентифицировать пользователя или ЭВМ достаточно сложно. Даже такие информативные признаки как IP или MAC-адрес могут быть недостоверными (нарушитель может использовать прокси-сервер или другой способ маскировки). Таким образом, для повышения точности идентификации необходимо использовать информативный набор признаков, на основе которого на этапе обучения формируются информационные образы внутренних пользователей (потенциальных нарушителей) или выявленных внешних нарушителей.

Известные подходы к идентификации (распознаванию) нарушителя по признакам работы на средствах вычислительной техники, основаны, как правило, на статистических методах. Такие методы хорошо работают при известных законах распределения признаков пользователя, возможности получения достаточно больших выборок значений признаков как на этапе обучения, так и в ходе идентификации, что на практике не всегда достижимо.

В условиях неопределённости априорной информации о признаках пользователей целесообразно использовать методы искусственных нейронных сетей.

Основными проблемными задачами, возникающими при использовании нейронных сетей в задаче идентификации нарушителя, являются определение информативного набора признаков пользователей, выбор типа нейронной сети и ее обучение. Результаты исследований возможности использования методов нейронных сетей, проведенных с помощью программного пакета Matlab, показали перспективность данного направления.

Предлагаемый подход позволяет реализовать высокий уровень автоматизации задачи идентификации нарушителя, в целом существенно повысить эффективность идентификации пользователя по показателям точности и оперативности. Также данный подход может быть использован для реализации дополнительного механизма аутентификации в инфокоммуникационных системах с высокими требованиями к защите информации от несанкционированного доступа.

Авраменко В.С., Деньжонков К.А., Чирушкин К.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВОЕННО-УЧЕБНОГО ЗАВЕДЕНИЯ

В настоящее время в Вооруженных Силах осуществляется переход на обучение по электронным учебникам, основой которого является электронная библиотека (ЭБ) военно-учебного заведения (вуз).

Электронная библиотека – информационная система, предназначенная для организации, хранения и использования электронных объектов (электронных образовательных ресурсов), объединенных единой идеологией комплектования, структуризации и доступа, с едиными средствами навигации и поиска.

Электронный образовательный ресурс – образовательный ресурс, представленный в электронно-цифровой форме и включающий в себя структуру, предметное содержание и метаданные о них.

Создание и применение ЭБ в процессе образовательной деятельности вуза требует осуществления комплекса организационно-технических мероприятий. Основными проблемными вопросами являются следующие: структура, состав и функции ЭБ, учитывающие особенности конкретного вуза; порядок комплектования фонда ЭБ; порядок доступа к электронным образовательным ресурсам, регламент работы с электронными образовательными ресурсами, содержащими информацию ограниченного доступа; вопросы обеспечения функционирования (технического, программного, информационного, нормативно-правового, кадрового и др.).

Электронная библиотека как библиотечно-информационная система, как правило, включает фонд электронных учебников и учебных пособий, каталог, модули регистрации пользователей и управления контентом, средства обеспечения сохранности и доступа. Также целесообразно реализовать функцию сбора и анализа статистики использования ЭБ (с целью контроля использования электронных учебников, оценки их востребованности, совершенствования таких сервисов ЭБ, как личный кабинет, интеллектуальный поиск и представление контента и др.).

Так как ЭБ каждого вуза может иметь свои характерные особенности (например, несколько вариантов размещения электронных образовательных ресурсов, удаленные территории), то необходима разработка локального правового акта вуза по организации ЭБ - «Положения об электронной библиотеке вуза», определяющем порядок ее создания и функционирования, а также учитывающим особенности ЭБ конкретного вуза. Каждый вуз может дополнять и расширять Положение в соответствии с особенностями вуза.

Также каждый вуз может разрабатывать дополнительные локальные нормативные правовые акты и документы по организации применения ЭБ – инструкции пользователям ЭБ, обязанности операторов и администраторов ЭБ, правила работы электронных читальных залов, графики и регламенты работы электронных читальных залов и др.

Направлением дальнейший работы по переходу на обучение по электронным учебникам является создание единого пространства электронных образовательных ресурсов в интересах всех вузов, обеспечение доступа обучающихся к ЭБ других вузов, ведущим электронным библиотекам Российской Федерации.

Анистратов И.В., Калюка В.И., Морозов Д.А.
Россия, г. Краснодар, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,
Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АЛГОРИТМИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ АНАЛИЗА СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА

В настоящее время активно продолжается развитие сетей широкополосного радиодоступа (СШРД) различной ведомственной принадлежности. Однако, наряду с известными научно-техническими достижениями в данной предметной области, благодаря изначально заложенной взаимно отличающейся технологической основы независимого существования СШРД, остается до конца не решена проблема оперативного доступа абонентов к общему информационно-телекоммуникационному ресурсу в любое время и в любом месте за счет технологической «бесшовности», обеспечивающей горизонтальное (внутрисетевое) и вертикальное (межсетевое) взаимодействие в информационно-телекоммуникационных системах (ИТКС).

Соответственно, оперативно решая частные задачи анализа СШРД с помощью средств программно-алгоритмической поддержки (СПАП), входящих в соответствующие системы поддержки принятия решений (СППР), за счет алгоритмических преобразований, направленных на минимизацию времени вычислений и повышения их точности, появляется возможность принятия обоснованных и своевременных управленческих решений при сокращении общего цикла управления в ИТКС. В свою

очередь, разработанные и внедренные СППР, позволяющие осуществлять поиск, распознавание и обработку информации, предсказательное (ситуационное) моделирование, не являются адаптивными, не способны отслеживать текущую ситуацию, не способны к сокращению времени вычислительных процедур. Поэтому, прежде всего, следует повысить эффективность вычислений в ходе решения оптимизационных задач за минимально допустимое время при выполнении требований по точности. Выполнение условий минимизации времени возможно при наличии эффективных СПАП, установленных на современных ПЭВМ. Условием достоверных и точных вычислений являются актуальные исходные данные, оперативно поступающие на вход СПАП в СППР для обработки и выдачи результата.

В целях оперативного решения задач анализа СШРД в СППР фиксируются вычислительные ресурсы (в соответствии с наличием СПАП) и требования по скорости и точности вычислений (в ходе алгоритмических преобразований), а эффективность принимаемых решений при планировании СШРД оценивается после вычисления показателей устойчивости, отражающих степень приспособленности СШРД к экстремальным условиям.

К внутренним свойствам, отражающим способность СШРД перестраиваться (адаптироваться) к изменяющимся условиям (требованиям, доступным ресурсам) и рассчитываемых при анализе, относятся:

- расширяемость, которая означает возможность сравнительно простого добавления отдельных элементов СШРД (абонентов, компьютеров, приложений, сервисов), наращивания длины сегментов СШРД и более мощных технических средств;
- масштабируемость, которая означает, что СШРД позволяет наращивать количество базовых станций и протяженность связей в очень широких пределах, при этом производительность СШРД не ухудшается;
- прозрачность, которая определяет свойство СШРД скрывать от абонента детали своего внутреннего устройства, упрощая тем самым его работу в СШРД;
- управляемость, которая подразумевает возможность централизованно (или децентрализовано) контролировать состояние основных элементов СШРД, выявлять и разрешать проблемы, возникающие при работе СШРД, выполнять анализ производительности и планировать развитие СШРД;
- совместимость, которая означает, что СШРД способна включать в себя самое разнообразное программное (алгоритмическое) и аппаратное обеспечение.

В значительной степени указанные выше внутренние свойства отражают способность СШРД приспосабливаться к изменяющимся условиям функционирования и наиболее ярко проявляются в значениях внешних сетевых характеристик, в определенных типовых или экстремальных ситуациях. Они учитываются в ходе алгоритмических преобразований, направленных на повышение вычислительной эффективности алгоритмов при решении частных задач анализа СШРД.

Апарина Е.Ю., Зубакин В.В.,Сазонов В.В., Титов В.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АВТОМАТИЗАЦИЯ ПЛАНИРОВАНИЯ И ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ПОЛЕВОЙ СИСТЕМЫ ОБМЕНА ДАННЫМИ ТАКТИЧЕСКОГО ЗВЕНА

Система обмена данными (СОД) тактического звена представляет собой поканальную физическую связность комплектов аппаратуры передачи данных (АПД) из состава телекоммуникационного оборудования комплексных аппаратных связи (КАС), командно-штабных (КШМ) и специальных машин (СМ) на пунктах управления соединения, батальонов (дивизионов), рот (батарей), взводов (расчетов) и т.д.

Кроме того, следует учитывать логическую связность, которая для современных телекоммуникационных средств может быть представлена в виде туннелей для передачи данных, необходимость и количество которых определяется потребностями непосредственного информационного обмена между должностными лицами (ДЛ) органов управления.

Практическая реализация принятых решений на этапе планирования и в ходе оперативного управления СОД предполагает их оформление в виде, необходимом при генерации АПД для работы в полевой сети передачи данных (СПД). Обычно решения по организации СПД представляются в форме рабочей документации, которая включает маршрутно-адресные документы (МАД) и задания боевым постам.

Исходными данными для планирования полевой СПД являются распоряжение по связи (и автоматизации) вышестоящего органа управления; указания начальника штаба по организации управления; имеющийся комплект средств передачи данных и выделенные каналы транспортной сети. На основе этих исходных данных разрабатывается маршрутно-адресная информация (МАИ), в которой должна быть определена физическая, адресная, ключевая и логическая структура сети.

Для функционирования аппаратуры унифицированного комплекса средств передачи данных, используемого в перспективных КАС, КШМ и СМ требуется разработать МАИ, которая содержит генерационную информацию для каждого комплекта АПД о топологии сети связи, типе и режиме работы подключенных каналообразующих средств. Формализованная МАИ включает:

- таблицы конфигурации комплекта (ТКК);
- таблица физических каналов (ТФК);
- таблица соответствия позывных приемника АПД IP-адресу прокси-сервера (туннельному адресу) на указанном канале (ТТА);
- таблицы базовой топологии сети (ТБТ);
- таблицы векторов связности абонентов (ТВ);
- таблицы соответствия адресов (ТСА): IP-адреса и сетевого адреса;
- таблицы подмены адресов АВСКУ-ООД (ТПА);
- таблицы номеров криптонаправлений (ТНКН);
- таблицы логических каналов (ТЛК) или таблица маршрутов;
- таблицы ключей (ТУНК) – таблица учета номеров КД

Эти таблицы могут быть разработаны ручным или автоматизированным способом. Ручной способ разработки не позволяет своевременно за отведенное для планирования системы связи время разработать МАИ, учесть все тактико-технические особенности организации СПД, устранить ошибки при написании строк соответствующих таблиц.

При автоматизированной разработке МАИ обязательным атрибутом является ввод таблицы базовой топологии сети. При этом отпадает необходимость ввода таблиц ТЛК, ТВ и собственного адреса, формируемых автоматически в комплекте АПД.

Для автоматизированной разработки МАИ разработано специальное программное обеспечение (СПО) пункта управления связью (ПУС-Д), которое может быть установлено в АРМы начальника связи и офицера отделения связи. Это СПО обеспечивает комплексное автоматизированное решение основных задач по планированию и обеспечению функционирования всех подсистем системы связи соединения.

В частности, обеспечивается формирование совмещенной схемы организации связи и схемы СОД; распределение адресов между объектами системы связи; формирование и распределения настроечных данных (НД) телекоммуникационных средств; разработку документов плана связи; формирование радиоданных в виде унифицированных структур данных; планирование сетей шифрованной связи, телефонных сетей и СПД; формирование схем-приказов узлам связи, элементам УС и боевым постам; передачу НД по установленным каналам связи, дистанционный ввод маршрутно-адресной информации в АПД СОД.

В процессе функционирования СОД и системы связи в целом могут быть обеспечен автоматизированный контроль состояния элементов системы связи, модификация МАИ, формирование документов и отчетов

Дополнительно при организации СОД должны быть разработаны документы для обеспечения функционирования автоматизированных рабочих мест в КШМ, ШМ, КАС и выносных АРМ.

Бакунин С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ ОБМЕНА ДАННЫМИ

При передаче информации в системах обмена данными по каналам связи, образованным различными средствами связи, всегда возникают ошибки. Вероятность искажения бита в потоке на уровне физического канала находится в широких пределах. Причины, влияющие на процесс передачи данных, могут быть различными, но результат для них получается один – данные искажаются и, как правило, для дальнейшей работы не всегда используются приемной стороной. В этом случае большую часть времени приходится затрачивать на повторную передачу информации, что в свою очередь влияет на контрольные сроки прохождения информации и в частности на актуальность данной информации. Для устранения возникающих ошибок известно множество различных способов, которые можно разделить на две группы: использующие обратную связь и без обратной связи.

В случае без обратной связи передаваемые данные кодируются одним из кодов с исправлением ошибок на передающей стороне, а на приемной стороне происходит декодирование полученной информации и исправление обнаруженных ошибок. Способность исправления ошибок зависит от числа избыточных битов применяемого кода, если вносимая избыточность невелика, то есть опасность того, что принимаемые данные будут содержать необнаруженные ошибки, которые могут привести к ошибкам в работе прикладного процесса. Если же использовать код с высокой исправляющей способностью (большой избыточностью), то это приводит к необоснованно низкой скорости передачи данных.

В связи с этим более предпочтительными считаются коды с меньшей избыточностью, так как избыточность напрямую связана с эффективностью сети.

Также следует учитывать и то, что чем выше избыточность кода, тем сложнее и дороже должны быть кодирующие и декодирующие устройства, что является не менее важным фактором, чем допустим пропускная способность канала связи, поскольку стоимость оборудования должна соответствовать ее необходимости, то есть должна окупаться сравнительно быстро.

В системах с обратной связью применяются процедуры обнаружения ошибок и переспроса, также называемой решающей обратной связью или обнаружением ошибок с автоматическим запросом повторения (АЗП) и информационной обратной связью.

В первом случае код применяется только в режиме обнаружения ошибок, что позволяет достичь очень низкой вероятности необнаруженной ошибки при незначительном уровне вводимой избыточности.

Для реализации механизма АЗП передаваемые данные организуются в специальные блоки, которые называются кадрами. Каждый правильно принятый кадр может быть подтвержден отдельным специальным кадром, либо подтверждение может быть вставлено в управляющее поле информационных кадров, переносящих данные в обратном направлении. В последнем случае также должны применяться специальные кадры подтверждения, поскольку информационного кадра в нужный момент может не оказаться.

При передаче данных модемами наиболее широкое применение нашел подход, основанный на использовании методов АЗП. Иногда также применяется комбинация двух рассмотренных подходов, заключающаяся в реализации на передающей стороне сначала кодирования с обнаружением ошибок, а затем кодирования кодом с исправлением ошибок. Такие методы гибридного АЗП особенно эффективны при передаче данных по каналам очень низкого качества.

Системы с решающей и информационной обратной связью обеспечивают одинаковую достоверность. При возникновении ошибок, которые группируются в пакеты, предпочтительнее системы с информационной обратной связью, поскольку передача сообщений по обратному каналу происходит в более благоприятные интервалы времени, чем по прямому каналу. Однако системы с информационной обратной связью имеют более сложное техническое оборудование, а используемые в них каналы связи характеризуются меньшей пропускной способностью. Поэтому в действующих сетях чаще применяются системы с решающей обратной связью в сочетании с контролем на четность или циклическим кодированием.

Башкирцев А.С., Шинкарев С.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПЕРСПЕКТИВНЫЙ ОБЛИК АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СВЯЗЬЮ СИЛОВЫХ МИНИСТЕРСТВ И ВЕДОМСТВ

Современные системы связи, применяемые в силовых министерствах и ведомствах Российской Федерации, в общем случае предназначены для решения следующих основных задач:

- доведение с заданными вероятностно-временными характеристиками приказов, сигналов и команд управления;
- качественное и своевременное предоставление и должностным лицам органов управления силовых министерств (ведомств) инфо-телекоммуникационных услуг;
- выполнения требований устойчивого, непрерывного, оперативного и скрытного управления силами, находящимися в подчинении силовых министерств (ведомств).

Основной компонентой любой системы связи, обеспечивающей эффективное выполнение вышеуказанных задач, является ее система управления.

Текущий уровень развития систем управления связью с учетом существующих тенденций наращивания «глубины» автоматизации процессов управления связью позволяет определить типовой перспективный облик автоматизированной системы управления связью (далее - АСУС) силовых министерств (ведомств).

АСУС, являясь основным инструментом многоуровневой поддержки принятия решений должностных лиц управления связью для обеспечения планирования, подготовки к применению по назначению, а также применения частей связи с выполнением необходимых требований по устойчивости, непрерывности, оперативности и скрытности должна строиться на основе следующих подсистем: организационная, оперативно-техническая, технологическая.

Подсистема организационного управления должна реализовывать целевые задачи функционирования системы связи путём планирования связи, управления построением системы связи и применением частей связи силовых министерств (ведомств).

Подсистема оперативно-технического управления должна решать задачи по управлению сетями и услугами связи во взаимодействии с подсистемами организационного и технологического управления

Подсистема технологического управления предназначена для решения задач контроля и изменение технического состояния средств связи (сетевых элементов) сетей связи.

Создание указанных подсистем должно базироваться на ряде основных принципов:

– принцип соответствия организационно-технической структуры АСУС организационно-технической структуре системы связи силового министерства (ведомства);

– централизованное управление с возможностью децентрализации функций управления системой связи и её элементами;

– принцип обеспечения опережающей готовности ресурсов АСУС по отношению к системе связи силового министерства (ведомства);

– принцип единства научно-технической политики и системотехнических решений (в том числе использование единой системы стандартов по техническому, информационному и программному обеспечению) при создании средств автоматизации для всех подсистем АСУС;

– принцип сопряжения с системами управления взаимодействующих сетей и систем связи.

Бегмахмудов И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ХОДЕ ПРОГРАММНО – ЦЕЛЕВОГО ПЛАНИРОВАНИЯ В СИЛОВЫХ СТРУКТУРАХ

В классификации программного обеспечения под понятием прикладное программное обеспечение понимается программное обеспечение, предназначенное для разработки и выполнения конкретных задач пользователя.

Прикладное ПО работает под управлением операционных систем и включает в себя пакеты прикладных программ и прикладные программы пользователя.

Основную часть прикладного программного обеспечения составляют пакеты прикладных программ (ППП) – комплекс программ, предназначенный для решения определённого класса задач по некоторой тематике.

Существует огромное количество ППП, охватывающих практически все стороны деятельности человека. Всё множество ППП можно разделить на два больших класса: пакеты общего назначения и специализированные пакеты.

В настоящее время в силовых структурах используются ППП общего назначения, к которым относят текстовые и графические редакторы, электронные таблицы, средства подготовки презентаций и т.п., в основном зарубежного производства, допущенные к использованию порядком, установленным законодательством РФ.

Использование однотипных программ всеми силовыми структурами решило проблему информационного обмена между ними, однако продолжает сохранять некоторую зависимость всех силовых структур от импортного программного обеспечения.

Гораздо сложнее обстоит дело с методо-ориентированными и проблемно-ориентированными ППП, относящимися к специализированному программному обеспечению.

Методо-ориентированные ППП характеризуются тем, что в их алгоритмической основе реализован какой-либо экономико-математический метод, используемый для решения задач.

К пакетам этой категории относятся программные средства, реализующие методы математического программирования (линейного, динамического, статистического и т.д.), сетевого планирования и управления, теории массового обслуживания, математической статистики и др.

Проблемно-ориентированными ППП называются программные продукты, предназначенные для решения сложных комплексов задач в конкретной функциональной области.

Для силовых структур ППП относящиеся к данным группам разрабатываются различными производителями, которые в разработке программного обеспечения руководствуются требованиями заказчика и собственными возможностями. В результате в большинстве случаев указанное ПО не согласуется не только между различными силовыми структурами, но и внутри одной силовой структуры.

Наиболее рациональными путями в решении возникших проблем по согласованию ППП остаются:

– стандартизация документальной базы между взаимодействующими силовыми структурами;

– использование унифицированных пакетов ППП;

– выбор единого перечня отечественных производителей программного обеспечения, отвечающих требованиям всех заказчиков;

– наращивание возможностей единой инфокоммуникационной сети силовых структур для организации единого информационного пространства.

Бернардо А.К., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

О ПРОБЛЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ СЛУЧАЙНЫХ ВОЗДЕЙСТВИЙ И АВАРИЙНЫХ СИТУАЦИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

К автоматизированным системам специального назначения (АС СН) предъявляются повышенные требования по обеспечению безопасности информации и устойчивости функционирования в различных условиях, что связано со значительными потерями, как ресурсными, так и финансовыми в случае нарушений в работе таких систем. Одним из ключевых моментов в выполнения данных требований является гарантия сохранности данных, что обеспечивает целостность и доступность информации, а также сокращение времени восстановления работоспособности системы.

В случае неопределенности множества угроз функционированию АС СН единственный способ надежно сохранить нужную информацию и обеспечить устойчивую работу органов управления – резервирование технических и программных средств. При этом системы резервного копирования и восстановления информации (РКВИ) являются основой защиты информации от случайных воздействий и аварийных ситуаций в любой системе с высокими требованиями к устойчивой работе, что делает системы РКВИ неотъемлемым инфраструктурным элементом АС СН. В настоящее время на рынке представлено множество готовых решений и методик резервного копирования и восстановления для корпоративных автоматизированных систем различного размаха, однако их применение в АС СН ограничено по ряду причин, обусловленных особенностями АС СН.

При внедрении систем РКВИ ответственным должностным лицам необходимо учитывать ряд особенностей функционирования АС СН: стремительное увеличение объемов хранимых данных; множество взаимосвязей задач, этапов управления, с характерной для них нагрузкой на сеть, при этом интенсивность потоков информации может резко меняться; выполнение значительной части задач в реальном масштабе времени; наличие различных приоритетов в решении задач и жесткие директивные сроки, а также характеристики рабочих мест и серверов в ЛВС.

Следует также учитывать, что сама система РКВИ является служебной подсистемой АС СН, не является критичной для решения задач управления, и нагрузка, формируемая в процессе ее функционирования на вычислительные средства и сеть, не является полезной. Следовательно, при настройке системы РКВИ требуется уложиться в довольно узкое «окно» бэкапа, то есть обеспечить минимальный временной интервал ограничений в работе системы, снизить трафик данных в процессе резервного копирования в сети, особенно в случае удаленности элементов АС СН друг от друга. Кроме того, при организации РКВИ в АС СН необходимо учитывать уровни конфиденциальности обрабатываемой информации, что накладывает дополнительные требования к РКВИ: разграничение доступа к резервным копиям, реализация механизмов защиты резервных копий от несанкционированного доступа, физическая защита хранилищ бэкапов, обеспечение резервного копирования зашифрованных данных, защита бэкапов в процессе передачи по сети, строгий аудит резервного копирования и восстановления.

Все вышеперечисленное говорит о том, что задача РКВИ является многокритериальной, ей должно уделяться достаточное внимание со стороны руководства организации, решением данной задачи должен заниматься высококвалифицированный инженерно-технический персонал под контролем службы информационной безопасности.

Бирюков М.А., Брунилин А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

УПРАВЛЕНИЕ РАЗГРАНИЧЕНИЕМ ДОСТУПА КАК ВАЖНЕЙШАЯ ЗАДАЧА ИНТЕГРАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЕДИНОМ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОМ ПРОСТРАНСТВЕ

Задача интеграции автоматизированных систем (АС) на базе единого информационно-вычислительного пространства (ЕИВП) становится все более актуальной. Ввиду этого возникает проблема защищённости ЕИВП от несанкционированного доступа (НСД) Для анализа этой проблемы необходимо определить угрозы безопасности информации, хранимой интегрируемой в ЕИВП.

Появление новых информационных угроз безопасности как внутренних, так и внешних, постоянное совершенствование средств и методов ведения информационной борьбы ведущими странами мира обусловливает необходимость разработки и совершенствования, новых средств защиты информации (СЗИ), а в частности, системы управления разграничением доступа к ресурсам ЕИВП.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными, и/или непреднамеренными воздействиями на нее.

В этом ключе под угрозой безопасности информации понимается любое событие (действие, ситуация), вызванное намеренно или непреднамеренно, которое способно неблагоприятно повлиять на ЕИВП по причине нарушения ее основных качественных характеристик (свойств).

Разработчики современных АС должны позиционировать их как системы, защищенные от внешних угроз. Поэтому, в работе предлагается ряд обязательных организационно–технических мероприятий, предусматривающий использование определенных механизмов позволяющих эффективно разграничивать доступ всем пользователям ЕИВП с учетом требований АС, интегрируемых в ЕИВП.

Богачев К.Г., Мещанин В.Ю.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ СЦИ НА ВНОВЬ ПРОЕКТИРУЕМЫХ СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ: СКРЫТЫЕ ПРЕИМУЩЕСТВА ИЛИ ОШИБКА ВЫБОРА?

Множество новых стандартов, введенных рабочей группой IEEE 802.3 за два прошедших десятилетия позволили технологии Ethernet стать технологией, удовлетворяющей требованиям большинства приложений. Ethernet, которая была технологией локальных сетей быстро заменяет устаревшие технологии, такие как СЦИ на сетях масштаба города, региона и в промышленных сетях. Индустриальные сети и сети приложений, традиционно тяготевших к СЦИ, а так же многие другие технологии в основной своей массе мигрируют к технологии Ethernet. Причин для этого много: простота, совместимость и экономическая эффективность. Сетевые приложения применяют технологию TDM поверх IP и мультисервисные Ethernet платформы.

Недавние усилия по стандартизации Ethernet были сосредоточены на улучшении QoS (качество обслуживания), OAM (эксплуатация, управление и техническое обслуживание). В результате технология Ethernet теперь способна обеспечить преимущества, которые ранее были доступны только СЦИ.

Сети на базе СЦИ были разработаны для того, чтобы использовать фиксированную полосу пропускания, а Ethernet гибкую. Природа мультиплексирования традиционного Ethernet представляет более эффективное использование полосы пропускания.

Основанный на Ethernet транспорт может удовлетворить потребности большего количества потребителей, при фиксированной общей емкости по сравнению с СЦИ, за счет грамотного распределения полосы пропускания и требуемого кратковременного превышения скорости для каждого потребителя.

Использование коммутаторов Ethernet в точках агрегации трафика вместо мультиплексоров ввода/вывода СЦИ позволяет значительно сократить расходы на строительство и эксплуатацию сетей связи. Недавно разработанные стандарты VCAT, LCAS, и GFP были призваны сделать технологию СЦИ более подходящей для передачи данных. Однако, Ethernet по-прежнему обеспечивает лучшую прозрачность, масштабируемость и большую степень детализации для обеспечения работы приложений.

Технология СЦИ применяет защиту n+1, что означает, разработанная для защиты сети пропускная способность используется только для защиты и не используется для переноса любого другого трафика. Для оперативного резервирования, Ethernet поддерживает протокол RSTP (IEEE 802.1w) и MSTP (IEEE 802.1s), которые предлагают балансировку нагрузки между рабочей и защищаемой сетями для более эффективного использования ресурса сети. Кроме того, в последнее время были разработаны решения, позволяющие строить сети Ethernet на кольцевых структурах, что еще больше повышает устойчивость их функционирования.

Большинство сетей СЦИ развернуты на кольцевых и линейных структурах. Причем всё свое преимущество технология СЦИ может реализовывать только на кольцевых структурах.

Отдельным вопросом стоит проблема синхронизации. Так, технология СЦИ может функционировать с заданными параметрами качества только при наличии сигнала синхронизации $\pm 10^{-5}$ ppm, в противном случае она переходит в асинхронный режим функционирования, что является аварийным состоянием сети. Сеть Ethernet изначально создавалась для передачи асинхронного трафика и поэтому для нормального функционирования оборудования сети достаточно иметь относительную точность частоты ±100 ppm. При этом для обеспечения потребителей синхросигналом необходимого качества разработано достаточное количество решений по переносу синхроинформации.

Кроме того в последнее десятилетие активно внедряется оборудование OTN-OTH/DWDM, которое является универсальным транспортом, позволяющим предоставлять гарантированную полосу пропускания для любых потребителей и реализовывать функции защитных переключений, тем самым избавляя наложенные сети от этой функции, что позволяет использовать оборудование Ethernet не поддерживающее кольцевые топологии.

Многие могут сказать, что существует ряд протоколов, позволяющих успешно передавать пакетный трафик через сеть СЦИ и эти протоколы превращают технологию СЦИ в СЦИ следующего поколения, но такое решение оказывается выгодным только в случае оптимизации использования уже существующего транспорта СЦИ. Использование СЦИ следующего поколения оправдано в первую очередь в контексте постепенного перехода от «классической» СЦИ к СЦИ следующего поколения.

Таким образом, можно сделать вывод, что решения заложенные с применением технологии СЦИ на сетях связи специального назначения и в аппаратных связи изначально являются технологически отсталыми, вводят дополнительный элемент ненадежности за счет введения дополнительного оборудования, осуществляющего передачу данных Ethernet поверх сетей TDM.

Болдырев П.А., Яцков А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ АКУСТИЧЕСКОЙ РАЗВЕДКИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ

Происходящие в настоящее время процессы в политической и экономической жизни России оказывают непосредственное влияние на состояние ее информационной безопасности. В современных условиях информация играет решающую роль как в процессе экономического развития, так и в ходе конкурентной борьбы на внутреннем и внешнем рынках.

Успешное функционирование и развитие предприятий все больше зависит от дальнейшего совершенствования их деятельности в области обеспечения информационной безопасности в сфере производства, бизнеса и предпринимательства.

Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов любой страны.

Создание развитой и защищенной информационной среды является непременным условием развития современного общества, поскольку именно через нее реализуются угрозы национальной безопасности в различных сферах деятельности государства.

Одним из источников конфиденциальной информации организации являются совещания, на которых проходит обсуждение этих вопросов. Присутствие большого количества ставят перед этими организациями проблему сохранения конфиденциальной информации.

Таким образом, защита информации при проведении совещаний с участием представителей сторонних организаций имеет актуальное значение и основными задачами по обеспечению информационной безопасности является выявление и своевременная локализация возможных технических каналов утечки акустической информации.

В качестве основных организационных мер по защите информации необходимо:

- проводить проверку помещения перед проведение совещания, с целью оценки состояния обеспечения безопасности информации;
- управлять допуском участников совещания в помещение;
- организовать наблюдение за входом в выделенное помещение и окружающей обстановкой в ходе проведения совещания;
- после проведения совещания комната должна тщательно осматриваться, закрываться и опечатываться.

В качестве основных технических мер по защите информации необходимо:

- в условиях совещания неуместно уменьшение громкости речи, поэтому для защиты такой информации следует применять звукоизоляцию, звукопоглощение и глушение звука для оконных проемов и дверей. Для обогревательных систем и вентиляции необходимо устанавливать экраны;
- для более надежной защиты информации рекомендуется установка подвесного потолка;
- установка комплексов виброакустической защиты и генераторов шума;
- вести оперативную проверку обстановки во время проведения конфиденциального совещания на предмет выявления закладных устройств, находящихся на одном из членов совещания или только что установленных.

Для обнаружения работающих диктофонов применять аппаратуру, позволяющей локализовать и максимально точно определить местонахождение закладки и ее потенциального обладателя.

Злоумышленник может получить конфиденциальную информацию через окна. Во избежании утечки акустической информации с помощью лазерного устройства съема информации со стекла, с помощью закладных устройств, а также с использованием направленных микрофонов, рекомендуется покрыть окна металлизированной пленкой.

Применение всего комплекса перечисленных организационных и технических мер по защите, обеспечит надлежащий уровень защиты акустической информации, циркулирующей в комнате для проведения совещания.

Боровкова М.А., Сидорова А.П., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТКРЫТОМ СЕГМЕНТЕ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ НА ОСНОВЕ КОНТЕНТ-АНАЛИЗА СЕТЕВОГО ТРАФИКА

В настоящее время идет активное оснащение органов государственного управления цифровыми узлами связи, обеспечивающими развертывание и функционирование локальных вычислительных сетей (ЛВС), предназначенных для предоставления инфокоммуникационных услуг должностным лицам органов управления, при этом ЛВС делится на открытый и закрытый сегменты в зависимости от грифа обрабатываемой информации.

В закрытом сегменте обеспечивается требуемый уровень безопасности информации, включая криптозащиту информации, передаваемой по каналам связи, защиту информации от несанкционированного доступа и технических средств разведки. В открытом сегменте политика безопасности предусматривает лишь наличие штатных, встроенных в операционную систему, средств защиты, а также средств антивирусной защиты и межсетевого экранирования.

В связи с тем, что информация, обрабатываемая в открытом сегменте, является служебной информацией ограниченного распространения, а обмен между сегментами осуществляется по каналам связи, предоставленным доверенными операторами, возникает задача контроля содержимого входящего и исходящего сетевого трафика или контент-анализ.

Система контент-анализа представляет собой набор политик, правил и фильтров для анализа входящего и исходящего трафика, при этом вся входящая и исходящая информация проходит через фильтр, который принимает решение о пропуске, задержке или блокировании пакетов, что дает возможность предотвратить угрозы не только утечки служебной информации, но и предотвратить угрозы спама, фишинга, вирусного заражения, атак на инфраструктуру и других негативных действий. Современные системы контент-фильтрации (СКФ) имеют развитый функционал, позволяющий настраивать фильтры в соответствии с задачами обеспечения безопасности для контроля почтового трафика и Web-трафика. В последнее время появляются новые области контент-фильтрации, такие как контроль VoIP-трафика, peer-to-peer соединений, а также контроль передачи шифрованных данных.

Наиболее востребованными для открытого сегмента инфотелекоммуникационной сети функциями систем контент-анализа (контент-фильтрации) могут являться: контроль отдельных пользователей (фильтры на принадлежность пользователя к определенной группе), фильтры на получателя информации (направление передачи данных), фильтры на отправителя информации, фильтры на содержание определенных словосочетаний, символов и конфиденциальных слов (контроль передаваемых текстов), а также проверка разрешений на передачу информации за пределы ЛВС.

Для качественного и полного решения задачи контент-фильтрации в открытом сегменте сети необходимо учитывать многие факторы: это особенности реализации СКФ, особенности построения и функционирования сети, взаимодействие с установленным программным обеспечением, методы работы пользователей, требования по обеспечению доступности ресурсов, взаимодействие с другими средствами защиты информации.

Таким образом, задача реализации в открытом сегменте инфотелекоммуникационной сети систем контент-анализа сетевого трафика является актуальной, перспективной с точки зрения обеспечения информационной безопасности, но требует дополнительных исследований в связи с рядом особенностей функционирования таких сетей.

Богаченко Д.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ЧИСЛЕННЫХ МЕТОДОВ ДЛЯ РЕШЕНИЯ ЗАДАЧ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ АНТЕННЫХ СИСТЕМ

В последние годы основным направлением развития проектирования радиоэлектронных систем является интеграция подсистем проектирования ориентированных на разработку специализированной радиоэлектронной аппаратуры в единую систему, поддерживающую процесс разработки устройств от СВЧ схем и антенн до цифровых схем обработки и формирования сигналов.

Состояние современной техники антенн предполагает использование мощных программных пакетов автоматизированного анализа при проектировании достаточно сложных антенных систем. Такое использование позволяет проводить параметрическую оптимизацию конструкции проектируемой системы ещё на этапе моделирования, избегая многократного макетирования.

Задачи, возникающие при проектировании современных антенных систем, требуют для своего решения применения новых методов анализа и синтеза как всей системы в целом, так и отдельных её узлов. В настоящее время на практике применяется множество пакетов точного трёхмерного

моделирования с применением метода моментов, метода конечных элементов, а также метода конечных разностей во временной области.

Метод моментов (Method of Moments, MOM) основан на поверхностных токах. Анализируемая структура разделяется на металлические пластины и проводники. После того как структура определена, все проводники разделяются на отрезки проводников, а пластины разделяются на небольшие (по сравнению с длиной волны) участки. После этого для получившейся структуры создается система линейных уравнений. Через решение этой системы линейных уравнений вычисляются токи для каждого отрезка провода и участка пластины. После нахождения токов можно узнать электрическое поле в любой точке пространства через векторную сумму решений уравнений для каждого отрезка/участка. Однако добавление диэлектриков усложняет использование этого метода и увеличивает объем требуемой для расчета оперативной памяти ЭВМ.

В методе конечных элементов (Finite Element Method, FEM) вычисления производятся по всему объему. Рассчитываемая область разделяется на небольшие элементы, обычно треугольной или тетраэдрической формы, и представляется как сетка, состоящая из конечных элементов. В этом методе используется допущение, согласно которому поля постоянны внутри каждого элемента сетки. Поле в каждом элементе аппроксимируется полиномом небольшого порядка с неизвестными коэффициентами. Эти аппроксимирующие функции подставляются в вариационное выражение, которое выводится из уравнений Максвелла, и получающаяся в результате система уравнений решается для определения неизвестных коэффициентов. После того как коэффициенты найдены, поля внутри каждого элемента известны.

Метод конечных разностей во временной области (Finite Difference Time Domain, FDTD) основан на центрально-разностной дискретизации уравнений Максвелла во времени и пространстве.

В итоге мы получаем систему из шести конечно-разностных уравнений, являющихся основой FDTD алгоритма, который позволяет рассчитывать взаимодействия электромагнитных волн с трехмерными объектами.

Программы точного моделирования трёхмерных структур – это новый, активно внедряемый подход, который становится основным инструментом проектирования, существенно увеличивая скорость разработки новых антенн.

Богданов А.В., Котяшичев И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

БОРТОВАЯ ШИРОКОПОЛОСНАЯ АНТЕННА С КОМБИНИРОВАННЫМИ НАГРУЗКАМИ ДЛЯ БЛА

Беспилотные летательные аппараты (БЛА) появились в связи с необходимостью эффективного решения военных задач — тактической разведки, доставки к месту назначения боевого оружия (бомб, торпед и др.) и управления боевыми действиями. Миниатюризация вычислительных систем позволила создавать БЛА, у которых габариты, масса, а главное, стоимость на порядки меньше прежних. Целью исследования является проектирование и моделирование широкополосной антенны для КВ и УКВ диапазонов с комбинированными нагрузками для БЛА.

Заданием была определена платформа для проектов расчета антенны – БЛА Орлан-10. Данный многофункциональный БЛА стоит на вооружении ВС РФ, предназначен для выполнения широкого спектра сложных задач. Поскольку существует необходимость уменьшения массогабаритных показателей полезной нагрузки на данном БЛА, мною была рассмотрена малогабаритная малогабаритная радиостанция нового поколения Р-187П1.

При проектировании антенных систем на БЛА основными вопросами являются: конструктивная разработка самих антенно-фидерных систем, обеспечивающих работу радиосредств в заданном диапазоне рабочих частот и удовлетворяющих единой комплексной системе общих технических требований на аппаратуру военного назначения, учет специфики назначения объекта, его конкретной конструкции, габаритов, технических и оперативных требований.

Решение сформулированных проблем возможно путём использования многоэлементных антенных систем в виде антенных решёток, в основу которых положен малогабаритный широкополосный излучатель. Правомерность такого вывода подтверждает анализ технических характеристик существующих антенных систем и результаты проведенного патентного поиска по теме: «Малогабаритные антенные системы», которые показывают, что существуют оригинальные технические решения, минимизирующие весогабаритные показатели, обеспечивающие достаточную широкополосность и эффективность. Примером таких антенн являются плоские антенны. Они удобны в эксплуатации и легко транспортируются. В то же время применение традиционных направлений повышения диапазонных свойств антенн, например, переход в режим бегущей волны и использование положений теории проволочных антенн для уменьшения габаритов не обеспечивает комплексного решения поставленной задачи.

Выходом из этого положения является использование иных принципов построения излучателей и, в частности, принципа трансформации полей, предложенного в патенте RU2207670C1 от 2001 г

/10/. Техническим результатом данного предложения является создание антенны с расширенным диапазоном рабочих частот при высоком уровне согласования, высоким уровнем предельной мощности и низким уровнем кроссполяризованной составляющей поля.

Таким образом, с целью выполнения задания по проектированию и моделированию широкополосной антенны для КВ и УКВ диапазонов проведен первый этап исследований – патентный поиск по теме: «Малогабаритные антенные системы». Установлено, что существуют оригинальные технические решения, минимизирующие весогабаритные показатели, обеспечивающие достаточную широкополосность и эффективность. Для дальнейших исследований выбрана полосково-рупорная антенна, в которой используется принцип трансформации полей.

Бровин Д.Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПОСТРОЕНИЯ ТРАНСПОРТНЫХ СЕТЕЙ ПОЛЕВОЙ ВОЕННОЙ СВЯЗИ

Как известно, на сегодняшний день многие эксперты сходятся во мнении, что успешность военных действий в двадцать первом веке во многом определяется не огневой мощью, то есть концентрацией сил, а степенью воздействия на информационные ресурсы противника. Данный фактор имеет особое отношение с позиции уязвимости к пространственно-разнесенным телекоммуникационным система – линиям и сетям связи, представляющие в своей основе особо протяженные и многосвязные электрически структуры с открытым доступом для множества как прямых, так и косвенных противодействий.

Военная первичная сесть связи является основой систем военной связи, которые в свою очередь, представляют материально-техническую основу систем управления войсками и оружием. Снижение надежности и качества их функционирования под воздействием факторов различного рода дестабилизирующего воздействия, включая преднамеренные воздействия, неизбежно отражается на устойчивости связи, а потеря связи неизбежно ведет к потере управления.

Известно, что значительная часть из арсеналов современных видов и средств вооруженной борьбы нацелена на дезорганизацию работы первичных сетей военной и гражданской связи противостоящей стороны как на локальном, так и на глобальном – общесетевом и общесистемном уровнях.

В связи с выше изложенным к одной из приоритетных задач, не только военной, но и государственной значимости, может быть отнесена полная и объективная оценка функциональных возможностей современных средств противодействий и иных мешающих факторов в отношении военной и гражданской связи, с опорой на данные соответствующих эмпирических испытаний.

Большая часть из ныне существующих проблем в области военной связи связана с обеспечением требуемых оперативно-технических и иных показателей наиболее дорогостоящей и сложной в организационном, технологическом и эксплуатационном отношении в части военных первичных стационарных и мобильных – полевых сетей связи.

В силу организации военные первичные сети связи, состоящие из множества разнородных, согласованных между собой по различным электрическим параметрам технических средств: по видам сигналов, по пропускной способности, полосам частот, входным и выходным сопротивлениям, динамическим свойствам и прочим. Это приводит к неизбежным, а иногда и многолетним задержкам во внедрении в первичные сети связи современных и совершенных технологий и средств, ныне обеспечиваемых научно-технологическим прогрессом в области телекоммуникаций.

В отличии от гражданской сети связи отработка оптимальных решений в области военных комплексов связи и военных первичных сетей связи требует организации и постановки комплексных натуральных испытаний с целью количественной оценки и практической отработки множества частных и системных показателей, таких как помеха защищенность, электромагнитной совместимости, живучести, технической надежности, электрической и электромагнитной устойчивости и прочие. Это требует так же проведения сопоставительных испытаний, конкурирующих образцов военных комплексов связи перед выбором наилучших из них для последующего принятия на вооружение.

Вайчикаускас М.А., Мондикова Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КЛАССИФИКАЦИЯ ПРИНУЖДАЮЩИХ АТАК И СХЕМ ОТРИЦАЕМОГО ШИФРОВАНИЯ

Традиционные методы криптографии позволяют обеспечить так называемую семантическую безопасность, защищая передаваемую информацию от «прослушивания», но не могут обеспечить надлежащую защиту в случае, если атакуемый подвергается принуждающей атаке.

В контексте такой атаки злоумышленник имеет определенный ресурс воздействия на атакуемого, принуждающий его раскрыть исходное сообщения и ключи случайных значений, использованных в процессе шифрования.

Технология псевдовероятностного защитного преобразования информации, также известная как отрицаемое шифрование, позволяет получить одну и ту же криптограмму из двух различных сообщений, одно из которых является истинным и не подлежит рассекречиванию, а второе, являющееся ложным, может быть предъявлено злоумышленнику в случае принуждающей атаки.

Рассмотрим случай, когда злоумышленник имеет возможность перехватывать пересылаемые сообщения в момент передачи данных. Помимо криптограммы, к числу этих сообщений так же могут быть отнесены некоторые случайные значения или данные, передаваемые в процессе аутентификации корреспондентов. Если после завершения сеанса коммуникации злоумышленник, обладающий вышеозначенными данными, принуждает корреспондента к раскрытию секретного ключа или иной информации, то говорят, что речь идет о пассивной принуждающей атаке.

Другой тип принуждающих атак, называемый «активная принуждающая атака», подразумевает, что злоумышленник навязывает пользователю сеанс коммуникации в рамках криптосистемы, использующей протокол отрицаемого шифрования, а после его завершения принуждает одного из корреспондентов раскрыть сообщение и секретный ключ.

В общем случае для защиты от активных принуждающих атак принято использовать процедуры взаимной аутентификации, в ходе которых удостоверяются личности пользователей, что позволяет идентифицировать атакующего еще до начала передачи шифртекста.

В случае, когда к раскрытию секретной информации принуждается отправитель, такая атака называется принуждающей атакой на отправителя. В противном случае, говорят о принуждающей атаке на получателя. Если имеет место пассивная принуждающая атака, то злоумышленник в равной степени может оказывать принуждающее давление, как на получателя, так и на отправителя. Подобный тип атак называют двухсторонней принуждающей атакой.

Согласно данной классификации схемы отрицаемого шифрования также подразделяются на схемы с отрицанием получателя, схемы с отрицанием отправителя, либо схемы с отрицанием обеих сторон (двустороннее отрицание).

Известно, что любая схема отрицания отправителя может быть трансформирована в схему отрицания получателя и наоборот. Также известно, что если хотя бы один участник взаимодействия не атакован, с его помощью возможно трансформировать схему отрицания отправителя в схему двухстороннего отрицания.

Ванчугов А.Н., Грибков В.А., Федоров П.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СПОСОБ УПРАВЛЕНИЯ ВХОДНЫМИ ПОТОКАМИ СООБЩЕНИЙ, ИСПОЛЬЗУЮЩИЙ ИНФОРМАЦИЮ О СОСТОЯНИИ СЕТИ И ОБЕСПЕЧИВАЮЩИЙ ЗАЩИТУ ОТ ПЕРЕГРУЗОК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Проблема управления потоками сообщений в сети передачи данных (ПД) рассматривается во многих научных работах, которые ориентированы, в основном, на сети общего пользования. Пристальное внимание к данной проблеме основано на следующих основных положениях:

– эффективность применения сети ПД в значительной степени определяется качеством используемых способов управления потоками сообщений;

– разработка и совершенствование способов управления потоками сообщений ведет к повышению эффективности использования не только вновь создаваемых сетей ПД, но и уже действующих, на тех же комплексах технических средств.

При управлении доступом в сеть ПД, особенно в условиях большой загруженности или в аварийных ситуациях, можно, ограничивая входные потоки сообщений в зависимости от внутренней глобальной нагрузки, предотвратить перегрузку сети и тем самым улучшить эффективность ее функционирования. В научной литературе известны различные способы управления потоками сообщений при доступе в сеть ПД. Для сетей пакетной коммутации с дейтаграммным режимом работы к ним относятся изоритмический способ и способ ограниченного объема входного буферного запоминающего устройства автоматического коммутационного центра (АКЦ).

При этом следует отметить, что использование изоритмического способа приводит к заметному снижению пропускной способности в условиях неоднородных тяготений между различными парами АКЦ. А способ ограниченного объема относится к способам локального управления объемом поступающей в сеть через АКЦ нагрузки, так как он основывается только на учете состояния буферного запоминающего устройства этого АКЦ.

Кроме того, рассмотренные способы управления строятся на основе эвристических методов, что затрудняет анализ связи управления входными потоками с маршрутизацией и оценку эффективности предлагаемых решений. В связи с этим следует рассмотреть способ управления

входными потоками сообщений, использующий информацию о состоянии сети и обеспечивающий защиту от перегрузок и заданные вероятностно - временные характеристики.

В сети ПД автоматизированных систем специального назначения (АССН) при передаче потока сообщений время доставки не должно превосходить некоторой допустимой величины. При этом возникает задача ограничения входных потоков сообщений на АКЦ сети: для этого необходимо построить такой способ управления входным потоком, который в случае перегрузки обеспечил бы новое распределение потоков и при этом пропускаемый поток был максимальным.

Предположим, что источником задержек в сети являются только тракты передачи данных (ТПД), в сети нет ни потерь, ни увеличения объема информации. Пусть в сети действует некоторый способ маршрутизации, который каждому распределению входного потока ставит в соответствие единственный набор переменных маршрутизации на АКЦ сети. Текущее значение среднего времени задержки сообщения в сети возрастает с увеличением нагрузки на сеть. Считая, что в сети действует оптимальный способ маршрутизации, рассмотрим способ управления входным потоком, состоящий из процедур ограничения и увеличения величины потока.

Задача оптимального увеличения и ограничения входных потоков может быть описана математическими выражениями линейной зависимости и заключается в расчете среднего времени задержки сообщения в сети, расстояния между всеми парами АКЦ, величин минимальных и максимальных входных потоков, с учетом выполнения условия допустимого времени отправки сообщения абоненту.

Из этого следует, что каждый АКЦ измеряет свои величины входных потоков, значения которых записываются в таблицу и передаются на пункт управления. В зависимости от ситуации и выполнения условия по своевременной доставке сообщения осуществляется процедура ограничения потоков, либо их увеличения. При этом ограничение нагрузки осуществляется постепенно, то есть сообщения низкой категории срочности получают отказ на вход в сеть ПД раньше, чем сообщения высокой категории срочности.

Рассмотренный алгоритм управления очередями потока данных позволяет производить расчет текущего значения средней времени задержки сообщения в сети и исходя из этого регулирует нагрузку на сеть путем увеличения или ограничения потока данных. В современных условиях развития автоматизированных систем специального назначения применение предложенного способа управления входящими потоками сообщений позволит сократить время доставки сообщения между абонентами и увеличить пропускную способность сети передачи данных.

Васюков Д.Ю., Яцков А.В., Болдырев П.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МЕТОДИКА ВОЕННО-ЭКОНОМИЧЕСКОГО ОБОСНОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Высокие требования, предъявляемые к уровню защищенности информационно-телекоммуникационной сети (ИТКС), предопределяют необходимость проведения оценки эффективности систем защиты информации.

Определение эффективности СЗИ затруднено существующим нормативно-методическим обеспечением информационной безопасности.

Известно большое количество средств защиты информации, которые условно можно разделить на несколько групп:

- средства разграничения доступа к информации в автоматизированных системах;
- средства защиты информации при передаче ее по каналам связи;
- средства защиты от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
- средства защиты от информационного воздействия программ-вирусов;
- средства обеспечения безопасности хранения, транспортировки носителей информации и защиту их от копирования.

Однако, практический опыт показывает, что ни одно отдельно выбранное средство защиты информации не может защитить ИТКС от комплекса целенаправленных воздействий (компьютерных атак), а комбинация разнообразных средств защиты приводит к снижению эффективности защиты в целом из-за конфликтности параметров средств защиты. Поэтому наметилась тенденция к построению эффективных систем информационной безопасности и обоснованию, на этой основе, требований к средствам защиты.

Эффективность функционирования СЗИ зависит от множества взаимосвязанных факторов и, как правило, оценивается совокупностью параметров, находящихся в сложных конфликтных взаимоотношениях.

Учитывая специфику СЗИ, которая характеризуется высокой стоимостью и наличием ряда жестких требований к ее эффективности, в качестве критерия оптимальности на этапе

предварительного проектирования целесообразно использовать затраты на создание и эксплуатацию СЗИ.

Наиболее распространенным методом оценки эффективности СЗИ является метод ветвей и границ, относящийся к методам неявного перебора.

Для решения методом ветвей и границ конкретной задачи следует определить:

- способ представления подмножеств решений;
- схему и способ ветвления;
- алгоритм вычисления нижней границы;
- метод нахождения рекорда (если это возможно не только для одноэлементного множества).

Таким образом, как видно из военно-экономического обоснования, увеличение средств выделяемых на приобретение различных средств защиты от КА ведет к увеличению защищенности ИТКС. Однако, в определенный момент повышение финансирования никак не влияет на защищенность ИТКС.

Виноградов А.Б., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНФОРМАЦИОННЫЙ КОНТРОЛЬ ИЗМЕНЕНИЯ СОСТОЯНИЯ КОНТРОЛИРУЕМОГО ИНФОРМАЦИОННОГО ОБЪЕКТА

Важной компонентой состояния контролируемого объекта является неизменность / изменяемость его состояния. Для одних объектов к параметрам работоспособности и функциональности относятся качества неизменности состояния, для других объектов - динамика состояния как характеристика их эффективности. Во многих системах производства и жизнедеятельности параметрами контроля являются диапазоны безопасного жизненного цикла изделий, средств производства и человека. Для контроля состояния объекта строится информационная матрица параметров объекта, включающая параметры идентификации, описания, контроля, рабочие параметры по организации конфигурации матрицы. Применяемый подход позволяет отойти от конкретики объекта контроля и работать с описанием контролируемого информационного объекта независимо от его прикладной принадлежности, полноты описания, содержательных характеристик объекта. Контроль параметров информационной матрицы осуществляется без учёта предыстории её построения только по значениям параметров.

Механизм контроля состояния базируется на сравнении матрицы состояния контролируемого информационного объекта и матриц образа объекта, которых может быть от одной до нескольких, в зависимости от алгоритма контроля состояния, но хотя бы одна матрица образа объекта совпадает с матрицей состояния контролируемого информационного объекта. Пакет наблюдений состояний объекта может содержать набор разных состояний одного контролируемого объекта, относящихся к состояниям объекта в разные времена с изменённым состоянием относительно первоначально контролируемого. Для унификации описания многообразия объектов контроля, методологическое описание информационного объекта сочетает приёмы трафаретного и специфического описания с расстановкой акцентов по требуемым параметрам контроля.

Матрица состояния имеет числовые значения и позволяет применять стандартный аппарат матричных вычислений. Аналогом матричного представления контролируемого информационного объекта может быть векторное представление с применением векторной алгебры, что используется для анализа состояния объекта как более наглядное для некоторых видов информационного представления объекта. Алгоритмы и правила анализа первичной обработки контролируемого информационного объекта имеют дополнительное расширение, которое связано с оценкой конфигураций матриц без учета конкретных значений параметров матрицы, благодаря этому в правила анализа включены элементы основных методов обработки и распознавания изображений и их аппарат геометрических преобразований, в том числе методы сегментации, нормализации и распознавания. Приёмы сегментации широко применяются для первичного и блиц-анализа изменяемости состояния контролируемого информационного объекта, что позволяет на последующих этапах контроля снижать размерность решаемых задач и ранг матриц. Приемы сегментации позволяют снижать вычислительную сложность при высокой степени детализации или многомерности контроля, разбивать признаковые пространства информационного объекта при достаточности только фиксации изменения состояния с расстановкой флажков нахождения отклонений между матрицей состояния и образом объекта.

Применяемый подход к информационному контролю изменения состояния контролируемого информационного объекта использует максимально упрощённые приёмы анализа состояний объектов, но использует предварительную методологию информационного описания объекта и его образа с проработкой степени конкретизации и унификации объекта, его поведения и степени критичности возникающих изменений, что должно быть отражено в логике выявления состояний изменения объекта и последующих правил и алгоритмов их обработки.

Винокуров А.В., Махов Д.С.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

РАЗРАБОТКА ПРОГРАММНО-АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ АДАПТИВНОЙ ОБРАБОТКИ ВИДЕОИНФОРМАЦИИ НА БОРТУ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

В настоящее время технологии обработки видеосигнала развиваются высокими темпами. Исследования вопросов сжатия, защиты от ошибок и передачи видеоинформации в современных телекоммуникационных системах освещаются в научной и технической литературе достаточно подробно. При этом, методы и алгоритмы обеспечения требуемой достоверности и оперативности обработки и передачи видеоинформации в робототехнических комплексах, включая комплексы с беспилотными летательными аппаратами, в условиях преднамеренных помех являются недостаточными.

Актуальность исследования обусловлена как необходимостью адаптивного реагирование на состояние окружающей среды и помеховой обстановки в тракте передачи видеоинформации «БЛА – НПУ», так и необходимостью уменьшения объема передаваемой информации перед процедурой ее криптографической защиты, определяемой требованиями нормативных документов.

Таким образом, формулировка задачи заключается в снижении качества передаваемых видеоданных без снижения их ценностного аспекта для получателя.

Для решения поставленной задачи предлагается применение технологий искусственного интеллекта, в частности, построение искусственной нейросети.

Исходные данные: изображение, получаемое с бортовой аппаратуры БЛА; набор характеристик изображения, связанный линейной зависимостью со временем передачи на пункт управления.

Внешние управляющие воздействия: матрица ранжированных значений помеховой обстановки в радиоканале и показатели качества оптического канала «Борт – Земля».

Необходимо: осуществить обработку видеоинформации и ее передачу на пункт управления с максимальным качеством за минимальное время.

Для решения поставленной задачи предлагается построение и использование нейронной сети прямого распространения, состоящей из трех слоев (входного, скрытого, выходного). Веса на входном слое отражают качество сигнала и изменяются от 0 до 1, регулируются устройством анализа помех. Выходной сигнал нейросети поступает на блок сравнения, учитывающий ограничения по показателю Тз – время заданное.

При условии невозможности передачи изображения за время $t \leq Тз$ сигнал поступает на устройство анализа помех, которое снижает качество изображения до допустимого уровня путем регулировки весов нейронов, соответствующих каждому входному пикселю. При нулевом значении веса нейрона входного слоя пиксель не учитывается, что ведет к снижению качества передаваемого изображения.

Направлением дальнейшей работы является моделирование нейросети и проведение экспериментальных исследований; оценка временной и емкостной сложности алгоритма адаптации с учетом ограничений, накладываемых на программно-аппаратные ресурсы БЛА и временные ограничения на обработку видеоинформации; определение минимальных пороговых значений параметров видеоинформации.

Волков Д.В.
Россия, Санкт-Петербург Военная академия связи имени Маршала Советского Союза С.М. Буденного

МУЛЬТИАГЕНТНЫЙ ПОДХОД К ПОСТРОЕНИЮ ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ СВЯЗИ ОБЩЕВОЙСКОВОГО СОЕДИНЕНИЯ

Боевое применение системы связи общевойскового соединения определяют наиболее сложные условия функционирования, обусловленные высокой динамикой боя и резкими изменениями боевой обстановки. На этапе планирования связи в соединении выполняется подготовка к функционированию системы связи, формируются исходные данные, обуславливающие ее структуру и т.п.

Основная идея способа представления модели – отражение ее свойств и различных компонентов с точки зрения мультиагентного подхода (модель как совокупность взаимосвязанных агентов).

Предполагается, что читатель владеет такими понятиями, как агентный подход, имитационное моделирование и т.д.

Итак, разрабатываемая модель представляет собой программно-аппаратный комплекс для проектирования, разработки, реализации, эксплуатации и сопровождению моделей-агентов. Подразумевается, что модель будет запускаться в гетерогенной вычислительной сети, где происходит имитационный прогон, по результатам которого собирается статистика.

В общем виде процесс создания модели будет выглядеть следующим образом:

- описание модели;
- задание параметров модели;
- запуск и сбор статистики.

Основной задачей при построении модели является описание структуры и различных способов поведения агентов. Агенты самостоятельны, они могут сотрудничать друг с другом при принятии решения. Принятие решений достигается за счет множества взаимодействий агентов, которые практически невозможно отследить. В принципе это и не требуется, так как агентам ставятся цели, которых они должны достичь, но не предопределяют сценарии исполнении задач по достижению этих целей.

Эти сценарии формируются и исполняются агентами самостоятельно. На каждом этапе агенты рассматривают входы системы и реагируют на различные события (влияние противника на систему). Реакция на воздействие противника может быть самостоятельной, либо осуществляться во взаимодействии с оператором.

Таким образом, возникает результат самоорганизации системы за счет множества скрытых или явных условий, сложившихся в ситуации, в прогнозируемых момент времени или спонтанно, и также исчезает, но в процессе своего существования руководит работой всей системы.

Итак, мы увидели, что построение модели на базе мультиагентного подхода действительно является нетривиальным. Чтобы привести все вышесказанное в порядок и ввести систематизацию в определении сущности модели, следует ввести точное математическое определение этого понятия.

В дальнейшем мы увидим, что определение модели будет иерархическим, в котором будут содержаться все детали и тонкости реализации.

Таким образом, построение мультиагентной модели системы связи общевойскового соединения позволит спроектировать некую абстрактную платформу, на базе которой можно будет предложить массу различных реализаций.

Вольхин С.Д., Алашеев В.В., Пустошкин М.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ЗАДАЧИ МОНИТОРИНГА ПОМЕХОВОЙ ОБСТАНОВКИ С ЦЕЛЬЮ ФОРМИРОВАНИЯ ИСХОДНЫХ ДАННЫХ ДЛЯ ОЦЕНКИ ЭЛЕКТРОМАГНИТНОЙ ДОСТУПНОСТИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

Высокие требования управления ведомственными силами диктуют настоятельную необходимость всестороннего и полного информационного обеспечения должностных лиц органов управления с одной стороны, а с другой предъявляют жёсткие требования к ведомственной системе связи по безопасности.

В настоящее время задача мониторинга помеховой обстановки с целью формирования исходных данных для оценки электромагнитной доступности радиоэлектронных средств решается на основании учета статических, усредненных исходных данных. При этом не учитываются особенности того или иного района возможного использования радиоэлектронных средств. Более того, возможны ситуации когда плотность радиоэлектронных средств в одном районе может существенно возрастать в течении короткого интервала времени.

Погрешности существующих-«традиционных» методик мониторинга помеховой обстановки наиболее существенны в УКВ диапазоне работающих радиоэлектронных средств, особенно применительно к условиям городской высотной застройки.

Задача мониторинга может решаться на основании прогноза учитывающего количество, типы и тактико-технические характеристики дополнительного количества радиоэлектронных средств и порядок их применения.

Для учета эффекта высотной городской застройки, возможного прибытия, перемещения дополнительных радиоэлектронных средств предлагается организовывать и разворачивать систему радиомониторинга помеховой обстановки в каждом конкретном районе использования радиоэлектронных средств.

Анализ показывает, что для эффективного радиомоноторинга района система должна обладать рядом особенностей:

- необходимо наличие не одного, а «n» средств и комплексов радиомониторинга в одном районе, при чем увеличение данных средств от четырех до восьми существенно повышает уровень эффективности функционирования системы;
- для полного охвата всех имеющихся, с учетом возможного прибытия дополнительных, радиоэлектронных средств и их перемещения по всей площади района, средства и комплексы радиомониторинга должны (по возможности) равномерно распределятся по всему району, а в условиях высотной городской застройки дифференцированно;
- для достижения необходимой эффективности в комплексах радиомониторинга необходимо использовать програмно-аппаратные радиоприемные устройства;

– текущая информация о помеховой обстановке передается в центр анализа, в котором осуществляется ее обработка с требуемой периодичностью для формирования исходных данных, необходимых для оценки электромагнитной доступности радиоэлектронных средств.

Такой подход позволяет дифференцированно подходить решению задачи мониторинга помеховой обстановки с целью формирования исходных данных для оценки электромагнитной доступности радиоэлектронных средств.

Воробьев А.И., Колбанёв А.М., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КОДИРОВАНИЕ МАРКЕРОВ НА ПОВЕРХНОСТНЫХ АКУСТИЧЕСКИХ ВОЛНАХ

Одним из интенсивно развивающихся направлений интернета вещей является радиочастотная идентификация объектов (RadioFrequencyIdentificationDevice) – RFID,позволяющая идентифицировать помеченный объект при помощи специального устройства – метки(транспондера). Существуют несколько разновидностей транспондеров, реализованных по разным технологиям. Одним из перспективных направлений являются транспондеры на поверхностных акустических волнах (ПАВ), основывающихся на пьезоэлектрическом эффекте. Благодаря отсутствию источника питания срок их эксплуатации ограничивается только механическими повреждениями.

Для того, чтобы радиочастотный считыватель мог собрать информацию со всех радиометок в его поле, необходимо чтобы в алгоритмах работы системы радиочастотной идентификации была реализованапроцедура «антиколлизии», предназначенная для разрешения ошибок, вызванных одновременным ответом нескольких меток на запрос считывателя, порождающим «коллизию», то есть ситуацию, когда считыватель не способен распознать принятые данные вследствие их наложения в радиоканале.

Выбор кодовых последовательностей для маркеров на ПАВ может быть сведен к формированию таких групп кодов, которые в совокупности (то есть каждый код группы с каждым другим кодом этой группы) отличаются друг от друга определенным числом разрядов. Чем большим числом разрядов отличаются коды, тем меньше их корреляция и наоборот. Уменьшение корреляции кодов внутри одной группы повышает вероятность правильного распознавания меток при одинаковом соотношении уровней сигнала и помех. Количественным показателем уровня корреляции является коэффициент корреляции.

Специфика поставленной задачи кодирования маркеров на поверхностных акустических волнах учитывается в применяемых алгоритмах и наглядно просматривается и подтверждает точность найденного решения.

Воробьев А.И., Колбанёв А.М., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ И ЕЕ ПРИМЕНЕНИЯ

Обобщенная модель устанавливает, что информационное взаимодействие должно изучаться с 3-х точек зрения:

1. с позиции коммуникантов, которые реализуют процессы мышления. Коммуникантам требуется определенное качество реализации информационных процессов обмена данными на материальном метауровне для эффективной поддержки интеллектуального взаимодействия на идеальном метауровне;

2. с позиции информационных процессов преобразования данных при помощи программно-аппаратных средств информационных технологий на материальном метауровне. Информационным технологиям требуются физические ресурсы, предоставляемые физической средой взаимодействия;

3. с позиции физических процессов, протекающих в среде взаимодействия и обеспечивающих преобразование данных. Физические процессы переноса сигнала во времени, в пространстве и обработка сигнала требуют энергии.

Обобщенная модель позволяет структурировать решение многих практических задач и нацеливает на комплексное изучение информационного взаимодействия. Ее значение вытекает из следующих обстоятельств:

– эффективность создания и использования интеллектуального потенциала на идеальном метауровне зависит от организации информационных процессов преобразования данных на материальном метауровне;

– эффективность информационных процессов материального метауровня зависит от используемой информационной технологии;

– эффективность информационных технологий определяется как их способностью поддерживать интеллектуальное взаимодействие на идеальном метауровне, так и от объемов потребляемых ресурсов на уровне физических процессов;

– эффективность функционирования физической среды взаимодействия определяется объемом потребления физических ресурсов по отношению к реализованным информационным и интеллектуальным процессам.

Обобщенная модель информационного взаимодействия показана на трёх примерах её использования:

– для выявления направлений развития информационной отрасли,
– выделения образовательных направлений в области информационных наук,
– классификации методов защиты информации.

Воронков К.Л., Рожнов М.Д., Шерстюк Ю.М
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

АРХИТЕКТУРА СОВРЕМЕННОЙ КОМПЛЕКСНОЙ СИСТЕМЫ МОНИТОРИНГА ИНФОТЕЛЕКОММУНИКАЦИЙ

Любую современную инфотелекоммуникационную сеть с позиций мониторинга можно рассматривать как систему образованную множеством объектов мониторинга (ОМ), состояние и функционирование которых представляют интерес в контексте решения задач управления, а также автоматизированную систему управления (АСУ), осуществляющую функции мониторинга контроля и управления по отношению к указанным объектам.

Важной составляющей указанной АСУ является система мониторинга, обеспечивающая оперативный и ретроспективный параметрический и событийный (фактографический) мониторинг, как постоянный (периодический) процесс сбора данных от потенциально неопределенного множества ОМ.

Оперативный мониторинг предполагает сбор данных мониторинга в интересах оперативного контроля состояния системы и ее компонентов, а ретроспективный в интересах аналитической обработки данных состояния и функционирования системы.

По отношению к каждому ОМ имеется один или несколько источников данных мониторинга (ИДМ), способных предоставлять данные о его состоянии и функционировании. Конструктивно ИДМ может быть интегрирован с ОМ (одним или несколькими) или функционировать отдельно от ОМ, осуществляя получение данных о состоянии / функционировании ОМ посредством взаимодействия с ним, а также предоставлять данные по нескольким.

Данные мониторинга в общем случае делятся на группы (параметрические и событийные) и подгруппы, определяемые для каждого класса ОМ.

Систему мониторинга инфотелекоммуникаций целесообразно строить как распределенную систему, образованную множеством программных средств – контроллеров данных (КД) и средств сбора и хранения данных (ССХД), осуществляющих управление КД. В общем случае КД должен обеспечивать получение данных мониторинга от ИДМ и передачу данных ССХД. Контроллер должен производить все необходимые вычисления на множестве получаемых данных от ИДМ и осуществлять передачу ССХД только изменения данных.

КД может быть локальным или удаленным как по отношению к ИДМ, так и по отношению к ССХД (локальность означает информационное взаимодействие в рамках одной локальной вычислительной сети).

Конструкция КД должна предусматривать возможность его одновременной работы с двумя и более источниками данных – однородными или разнородными.

Работа с разнородными источниками должна достигаться такой архитектурой КД, при которой реализуется инвариантная часть, обеспечивающая тракт управления контроллером, отправку данных мониторинга соответствующим ССХД, а также являющаяся среды погружения для модулей, обеспечивающих информационное взаимодействие с источниками данных определенного типа.

Таким образом, на уровне КД должен быть обеспечен единый механизм сбора и промежуточного хранения данных (буферизации), проведения необходимых расчетов и передачи данных мониторинга.

ССХД предназначены для получения данных мониторинга от подчиненных КД, их хранения и предоставления необходимых предметных данных другим подсистемам – потребителям.

Для обеспечения указанной целевой задачи в рамках ССХД должны осуществляться регистрация заданий на сбор данных контроля в форме наборов данных мониторинга, регистрация контролируемых КД, дистанционное управление параметрами их функционирования и выполняемыми ими заданиями.

С целью обеспечения контроля функционирования ССХД должны осуществлять периодический контроль факта функционирования КД и интерактивное отображение сведений о зарегистрированных КД, их функционировании и выполняемых ими заданиях.

Для построения системы мониторинга предлагается использовать архитектурный стиль REST (Representational State Transfer), позволяющий реализовать многоуровневую архитектура, обеспечивающую производительность, масштабируемость, модифицируемость, видимость, мобильность и надежность распределенной системы мониторинга.

Воронков К.Л., Курилов Д.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек Балтика»

УНИФИКАЦИЯ СРЕДСТВ УПРАВЛЕНИЯ СОВРЕМЕННЫМ ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ

Современное телекоммуникационное оборудование (ТКО) в абсолютном большинстве случаев имеет в своем составе программных агентов управления, способных осуществлять информационное взаимодействие с внешним по отношению к оборудованию программным обеспечением. Такое внешнее программное обеспечение относится к программным средствам мониторинга и управления оборудованием уровней EMS или NMS логической архитектуры, предусмотренной TMN (далее – средства управления).

В общем случае средства управления должны обеспечивать мониторинг функционирования оборудования (состояние, конфигурация, статистика, события и т.д.) и управление им – как управляющие воздействия, направленные на изменение состояния, параметров и режимов работы (как правило – через изменение параметров конфигурации оборудования).

Реализация функций мониторинга и управления в отношении ТКО предполагает взаимодействие с агентами управления ТКО с использованием одного или нескольких протоколов взаимодействия, поддерживаемых агентом управления ТКО. Среди основных протоколов, реализуемых агентами управления современного ТКО, наибольшее распространения получили:

1) Протоколы, обеспечивающие интерфейс командной строки (англ. cmd - command line interface). Обычно такой интерфейс обеспечивается протоколами telnet и ssh.

2) Протокол SNMP (англ. simple network management protocol — простой протокол сетевого управления), базирующийся на применении MIB (англ. management information base - база управляющей информации). Данный протокол предполагает чтение / запись скалярных и табличных параметров MIB, а также формирование и отправку агентом управления предусмотренных в MIB извещений (notifications, traps).

3) Протоколы, основанные на обмене файлами – например, sftp, ftp, ftps, tftp, ssh, scp, rsync. Они, в частности, позволяют обновлять программное обеспечение оборудования, изменять его конфигурацию, а также получать список произошедших событий из файлов журналов событий.

4) Протоколы http и https, позволяющие осуществлять мониторинг и управление ТКО через web-интерфейс http-сервера, встроенного в ТКО.

5) Протоколы, обеспечивающие использование встроенной в ТКО или внешней по отношению к нему службы syslog (англ. system log — системный журнал) для регистрации сообщений о происходящих в ТКО событиях.

Средства управления должны унифицировать взаимодействие с ТКО посредством предоставления пользователям (людям, программам) три интерфейса – параметрический и событийный для получения данных мониторинга ТКО и управляющий – для оказания управляющих воздействий на ТКО. Это означает, что в средствах управления целесообразно реализовывать унифицированные событийно-параметрическую информационную модель ТКО и модель воздействий на основе функций управления. Тогда функциональные действия в рамках этих моделей должны трансформироваться в интеракции с агентом управления с применением одного или нескольких вышеперечисленных протоколов. Существенно, что указанные модели в общем случае являются алгоритмически и информационно взаимосвязанными – выполнение функции управления может порождать событие и приводить к изменению значения одного или нескольких параметров, событие может трактоваться как изменение параметра и наоборот – изменение параметра порождать событие.

На унифицированные средства управления, обеспечивающие автоматизированный интерфейс мониторинга и управления по отношению к ТКО, также может быть возложено решение задач преобразования данных мониторинга в рамках используемой параметрической модели ТКО – преобразование типов данных, вычисление значений параметров, производных от первичных параметров мониторинга и так далее.

Таким образом, возможно построение формальной модели унифицированных средств управления современным ТКО с вариантным наполнением в части протоколов непосредственного взаимодействия этих средств с агентами управления в составе ТКО.

Вотинов М.Л., Уйманов А.В., Пустошкин М.М., Репников А.Ю.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОЦЕНКА ДОСТУПНОСТИ ДЛЯ НАРУШИТЕЛЯ ЗАЩИЩАЕМЫХ РЕСУРСОВ СИСТЕМЫ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТЬЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Одним из основополагающих моментов решения проблемы влияния информационных атак на систему управления телекоммуникационной сетью специального назначения (СУ ТКС СН) является оценка доступности защищаемых ресурсов системы управления от несанкционированного доступа нарушителя.

Во-первых, защищать от нарушителя необходимо и достаточно только такие сведения об информационных ресурсах СУ ТКС СН, которые (будучи вскрыты нарушителем) могут существенно снизить в условиях воздействия нарушителя эффективность функционирования системы управления.

Во-вторых, главное значение имеет свойство СУ ТКС СН скрывать от нарушителя оперативную информацию, передаваемую и хранящуюся в базах данных СУ ТКС СН, а также изменения в структуре и характере функционирования системы управления.

Эти выводы положены в разработку методов оценки и системы взаимоувязанных показателей защиты информационных ресурсов СУ ТКС СН от технической разведки и нарушителя.

В соответствии с существующей методологией оценки эффективности целенаправленных процессов при формировании системы показателей в ее состав должны быть включены показатели, характеризующие результативность (назначение), оперативность и ресурсоемкость оцениваемого процесса.

Показателями доступности для нарушителя объекта и его особо важных зон являются степень доступности в вероятностной шкале оценок (пример степеней: очень высокая, высокая, средняя, ниже средней, низкая) или экспертным путем на основе опыта специалистов.

Обратным показателем по отношению к показателю доступности является показатель устойчивости системы – степень защищенности объекта (зоны) или вероятность обезвреживания нарушителей до нанесения объекту ущерба.

Модель оценки представляет собой формализованный алгоритм расчета указанных показателей. Методика определяет порядок подготовки и ввода исходных данных, получения и представления результатов оценок.

Предлагаемая система показателей, включает показатели защищенности системы управления и ее ресурсов, непосредственно связанных с вероятностью реализации угроз безопасности, частные и обобщенный показатели эффективности функционирования СУ ТКС СН в условиях воздействия информационных атак.

Расчет показателей позволяет провести их оценку доступности ресурсов для нарушителя, а так же всей гаммы возможного изменения учитываемых аргументов, что позволяет сформулировать полученные требования к параметрам системы управления и разработать организационно-технические предложения направленные на повышение защищенности информации.

Васильева О.Н, Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МОДЕЛЬ ЭЛЕКТРОННОГО КОНСТРУКТОРА ДЛЯ ИЗУЧЕНИЯ СРЕДСТВ СВЯЗИ ПОЛЕВЫХ УЗЛОВ СВЯЗИ

Активное внедрение в систему обучения различных электронных программных аппаратных средств позволяет в ходе проведения групповых упражнений и практических занятий использовать ПЭВМ непосредственно в классе.

Оснащение военных вузов страны современными ПЭВМ компьютерными классами позволяет преподавателям проводить занятия с их использованием, при этом применять последние разработки в области программирования и моделирования.

В ходе проведения практических занятий по тактико-специальной подготовке слушатели и курсанты изучают принципы построения узлов связи, порядок их формирования, организационную структуру и пути прохождения сигналов (сообщений) на узлах связи, а также их размещения на местности и другие вопросы, связанные с изучением узлов связи.

В настоящие время указанные вопросы изучаются в ходе практических занятий с использованием традиционных методов в виде решений различных ситуационных задач. Ситуационные задачи решаются на подготовленных бумажных бланках или формализованной тетради.

С целью повышения познавательного процесса у обучаемых и внедрению современных инновационных технологий в подготовку слушателей и курсантов ходе тактико-специальной подготовки при изучении полевых узлов связи различных уровней управления необходимо разработать электронный конструктор (ЭК) «Полевые узлы связи».

Под вербальной моделью ЭК будем понимать абстрактную модель, содержащую описание требований, структуры, технологий, анализа использования данного программного продукта в учебном процессе, а также основные вопросы в процессе функционирования.

Подготовка модели ЭК должна осуществляться с изучения и уточнения требований, которыми должен обладать тренажёр.

Определяются задачи, которые должен выполнять тренажёр с учётом изучения дисциплины:

- изучение тактико-технических данных аппаратных и станций;
- выбор задания для выполнения;
- выбор режима работы;

- формирование организационно-технической структуры узлов связи;
- подготовка модели размещения узлов связи на местности;
- решение задачи по определению путей прохождения сообщения (сигналов).

Одной из сложной задачи по созданию ЭК является разработка аппаратно-программной оболочки и подготовка интуитивно-понятного пользовательского интерфейса тренажёра. В модели должен быть четко показан программный комплекс для разработки тренажера.

При подготовки пользовательского интерфейса и учебно-справочного материала, который в дальнейшем будет являться исходными данными, предлагается использовать графические и 3D-редакторы. Создаваемый при этом видеоряд обладает высокой реалистичностью. Применение указанных программ позволяет создать 3D модели аппаратных и станций применяющиеся при развёртывании узлов связи. Ядро ЭК должно формироваться модулями при этом каждый модуль может быть самостоятельным элементом тренажёра и быть блоком исходных данных для последующих модулей.

Состав модулей определяется их функционалом:

- «Тактико-технические данные аппаратных и технических средств связи».
- «Задание».
- «Формирование организационно-технических структур узла связи».
- «Размещение узла связи на местности».
- «Пути прохождения сигналов (сообщения)».
- «Геоинформационного моделирования УС на местности».
- «Виртуальный узел связи».
- «Оценочный модуль».

При разработке ЭК должна быть использована концептуальная модель с описанием её элементов. При этом создание модели позволило показать взаимосвязь самого интерактивного тренажёра с содержанием, требованиями, которые предъявляются к нему, технологии, использующиеся при его составлении, этапы его разработки и возможность его применения в различных видах занятий.

Используя представленную модель можно разработать техническое задание для непосредственной разработки ЭК с учётом всестороннего ее изучения.

Галаган А.О.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИССЛЕДОВАНИЕ ТРЕБОВАНИЙ И МЕТОДОВ ПРОКЛАДКИ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ В ПОЛЕВЫХ УСЛОВИЯХ

На данный момент оптоволоконные сети являются одним из самых перспективных и экономически выгодных способов соединения, удаленных друг от друга двух узлов сети. Они способны передавать большие массивы данных с меньшими потерями и практически невосприимчивы к электромагнитным полям.

Полевые оптические кабели применяются для прокладки в полевых условиях на поверхности грунта, в самом грунте, через водные преграды, при подвеске на местных предметах, а также в стационарных условиях. Кабель может использоваться многократно, обычно содержит от 1 до 12 оптических волокон.

Требования, предъявляемые к полевому кабелю, очень жестки. При легкости и малом диаметре он должен обладать стойкостью к многочисленным внешним воздействиям, например, таким, как раздавливающие нагрузки до 600 Н/см, растяжение с усилием до 10 кН, 100 циклов изгибов на диаметр, равный 10 внешним диаметрам кабеля; перемотки с барабана на барабан, закручивания, а также быть устойчивым к воздействию влаги, грызунов, агрессивных сред, бензина, керосина, дизельного топлива, отрицательным и повышенным температурам в диапазоне от -60 до +70°С. Кроме того, полевой кабель не должен распространять горение.

Одна из наиболее трудно решаемых задач для полевых оптических кабелей - задача одновременной устойчивости к раздавливающим и растягивающим нагрузкам. Проблема защиты оптического волокна от растяжения разрешается, в основном, путем его свободной укладки в трубке модуля (обеспечение небольшой дополнительной длины волокна). Стойкость к воздействию растягивающего усилия определяется бездеформационным (то есть только за счет распрямления) перемещением волокна внутри модуля. Однако наличие дополнительной длины может привести к появлению изгибов, способствующих увеличению затухания сигнала в волокне при воздействии на кабель внешнего давления и низких температур. Необходимо определить оптимальное значение запасной длины волокна. В настоящее время заметна тенденция к дальнейшему снижению массогабаритных характеристик полевых кабелей. Необходимость выполнения этих требований заставляет разработчиков отказываться от использования металлических армирующих элементов. Для защиты от растягивающих нагрузок в конструкциях применяются арамидные нити. Замена

металлических армирующих элементов на арамидные нити позволяет значительно улучшить характеристики полевых кабелей.

Обязательным требованием для полевых ОК является стойкость к воздействию гидростатического давления и влагостойкость. Влагостойкость подразумевает, что при прокладке в воде в течение всего срока службы воздействие влаги не приведет к значительному ухудшению передаточных характеристик ОК. Стойкость к воздействию гидростатического давления предполагает, что в течение 10 суток при воздействии гидростатического давления величиной в 1 атмосферу не произойдет распространение воды вдоль оси кабеля. Выполнение этого требования необходимо для предотвращения попадания воды в приемопередающую аппаратуру по поврежденному кабелю, расположенному в воде, в течение некоторого периода времени, необходимого для удаления и замены кабеля.

Таким образом, к полевым оптическим кабелям предъявляются наиболее жесткие требования по сравнению с другими кабелями связи, поэтому при разработке конструкций полевых кабелей необходимо проводить предварительный теоретический расчет на предмет стойкости к растягивающим, раздавливающим, температурным воздействиям, а также расчет продольной длины проникновения.

Ганин П.А., Михалев О.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СИНХРОННОЕ ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ И СОСТАВЛЕНИЕ КАРТЫ ПО СТЕРЕОИЗОБРАЖЕНИЮ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ НАВИГАЦИИ В РОБОТОТЕХНИКЕ

Возможность навигации в реальной среде – базовое требование к автономному мобильному роботу. При решении задачи навигации роботу требуется отвечать на три вопроса: «Где я?», «Куда я хочу идти?», «Как туда попасть?». Для ответа на эти вопросы, необходимо знать, к какой координатной системе и какому окружающему пространству они относятся. Система координат и информация о положении предметов в ней называется картой. Реализация навигационной системы, которой заранее известны ориентиры или карта пространства, при наличии достаточно точных сенсоров, не представляет больших сложностей.

Построение карты при постоянно известном положении робота также в значительной степени решенная проблема. Гораздо сложнее решать эти проблемы одновременно, не зная заранее ни карты, ни положения робота.

Simultaneous localization and mapping (SLAM) – синхронное определение местоположения и составление карты. Задача SLAM связана с построением карты неизвестного пространства мобильным роботом во время навигации по строящейся карте. Раньше решения данной задачи были трудоемкими и дорогими, использовались специальные методы: точное машиностроение, высокоточные сенсоры, калибровочные точки.

Альтернативой является применение нескольких перекрывающихся сенсоров меньшего разрешения и совмещение пространственной информации от датчиков для получения более точных результатов. Например, возможно совместное использование лазерного дальномера, видео камеры и информации о повороте и скорости вращения колес для автономного робота.

В настоящее время методы решения задачи SLAM быстро развиваются. Это обусловлено увеличением производительности вычислительных машин, улучшением качества датчиков и появлением новых, а также развитием робототехники. Задача SLAM является очень важной, так как без ее решения весьма затруднительно создание по-настоящему автономного робота. На данный момент существует несколько основных подходов к решению этой задачи: EKF-SLAM, FastSLAM, DP-SLAM.

Для решения задачи навигации и построения маршрутной карты для мобильного робота была выбрана система ROS (Robot Operating System) - широко используемый в робототехнике фреймворк, основной концепцией которого является создание программного обеспечения, которое бы работало с различными роботами и периферией к нему. В рамках ROS, реализовано несколько алгоритмов SLAM: GMapping — реализация метода SLAM на основе данных от лазерного дальномера и одометрии робота; VSLAM — визуальный SLAM — реализация метода SLAM на основе методов компьютерного зрения.

Задача SLAM состоит из множества частей: нахождение ориентиров в пространстве, поиск их соответствий, вычисление местоположения, уточнение местоположения и положений ориентиров. Таким образом, появляется возможность комбинировать различные реализации отдельных алгоритмов и улучшать их по отдельности. Например, замена может потребоваться для работы на больших пространствах вместо работы в помещениях. SLAM может применяться как для 2D-, так и для 3D-перемещений.

Горчаков В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИССЛЕДОВАНИЕ ВОПРОСОВ ПОСТРОЕНИЯ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Последние десятилетия во всем мире сопровождаются появлением новых военных угроз, изменением характера войн и военных конфликтов.

Внедрение сетевых технологий в военную сферу направлено на повышение боевых возможностей вооруженных сил, но уже не столько за счет наращивания огневых, маневренных и других характеристик вооружения и войск (сил), а в первую очередь за счет сокращения цикла боевого управления. Эти обстоятельства вынуждают военное руководство ряда передовых стран, в том числе и России, проводить целенаправленное широкомасштабное реформирование национальных вооруженных сил.

В современных условиях ведения боевых действий управление соединениями и частями является таким же решающим фактором успеха, как количество и качество войск и оружия, и в значительной степени определяет успех в решении боевой задачи.

Задачи военной связи, требования к ней и принципы ее организации, как к обеспечивающей подсистеме единой системы управления войсками, определяются предназначением системы управления, решаемыми войсками задачами, а также условиями организации и ведения боевых действий. Создание (развертывание) системы связи заключается в организации средств связи различного назначения и типа в определенную, строго соответствующую данным условиям оперативной обстановки и задачам системы управления войсками и оружием, структуру. Состав системы связи определяется составом звена управления, решаемыми задачами, условиями размещения частей и подразделений, принятой в звене управления системой пункта управления, наличием и состоянием средств связи с учетом физико-географических условий района боевых действий. Системы связи всех звеньев управления строятся на общих организационных и технических принципах, сопрягаются между собой и обеспечивают взаимное использование каналов и средств связи.

Техническую основу системы связи, а, следовательно, и системы управления войсками и оружием составляют радиоэлектронные системы связи. С учетом этого каждая из воюющих сторон будет использовать разнообразные способы, применять различные силы и средства для дезорганизации управления противника и обеспечения устойчивого управления своими войсками и оружием. Неминуемо будет развернута острая и напряженная борьба за достижение превосходства над противником в области управления. Этот процесс является одним из видов боевого обеспечения и называется радиоэлектронная борьба.

Развёртывание системы связи и её модернизация - это объёмные задачи, требующие большого количества временных и трудовых ресурсов. Следовательно логично оценивать способность системы соответствовать поставленным требованиям до её развёртывания.

Расчёты позволяющие произвести оценку достаточно монотонны, их возможно стандартизировать и сделать более наглядными, используя современную вычислительную технику. Это позволит увеличить скорость принятия решения по расположению узла связи или техники в нем. Как следствие логично разработать приложение реализующее алгоритм расчета пропускной способности системы связи тактического звена управления. Такое приложение должно обладать способностью располагать на карте узлы связи, добавлять в них аппаратные средства и рассчитывать пропускную способность смоделированной системы с учётом рельефа местности.

Данилова Е.И., Зотов Д.Г., Ракицкий С.Н., Ракицкий Д.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МЕТОДИКА ОЦЕНКИ СВОЕВРЕМЕННОСТИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Большинство исследований в области контроля защищенности информации направлено на исследование контроля безопасности информации в части совершенствования характеристик отдельных его свойств.

Наряду с разработанными комплексами средств контроля защищенности информации на объектах информатизации, а также методик сетевого планирования контроля, вопросы оценки состояния защищенности информации на объектах информатизации не рассматривались, а предложения по составу комплекса средств контроля носили скорее рекомендательный характер.

Решение задачи по оценке своевременности контроля защищенности информации сводится к разработке методики оценки своевременности контроля защищенности информации от ее утечки по техническим каналам на объектах информатизации и разработке на их основе научно-технических предложений по совершенствованию процесса и системы контроля защищенности информации.

Несовершенство имеющегося научно-методического аппарата, проявляющееся в отсутствии возможности количественного обоснования требуемого ресурса сил и средств контроля на объектах информатизации, определяет необходимость разработки методики оценки своевременности контроля защищенности информации от утечки по техническим каналами на объектах информатизации и разработки предложений на их основе по составу сил и средств контроля защищенности информации.

Методика предназначена для оценки своевременности контроля защищенности информации от ее утечки по техническим каналам на объектах информатизации с заданной достоверностью.

Исходными данными для методики являются потоки заявок в систему контроля защищенности информации (бригаду) на проведение спецобследований объектов информатизации, получаемые из проведенного анализа требований руководящих документов по периодичности проведения спецобследований объектов информатизации различных категорий, количества бригад и личного состава в них.

Разработанный алгоритм методики оценки своевременности контроля защищенности информации от ее утечки по техническим каналам предусматривает следующую последовательность действий:

- производится ввод исходных данных;
- осуществляется расчет того, что все обслуживающие бригады (люди) свободны;
- осуществляется расчет вероятности того, что занято обслуживанием n бригад (людей);
- осуществляется расчет коэффициента загрузки приборов - бригад (людей);
- осуществляется расчет коэффициента простоя приборов - бригад (людей);
- осуществляется расчет среднего времени ожидания требованием начала обслуживания в системе контроля защищенности информации (в бригаде);
- осуществляется расчет среднего времени пребывания заявки в системе контроля защищенности информации (в бригаде);
- осуществляется расчет среднего времени пребывания заявки в очереди;
- осуществляется расчет среднего числа требований, находящихся в системе контроля защищенности информации (в бригаде);
- осуществляется расчет средней длины очереди на обслуживание;
- осуществляется расчет среднего количества занятых обслуживанием приборов - бригад (людей);
- осуществляется расчет среднего количества свободных от обслуживания приборов - бригад (людей);
- осуществляется расчет удельной нагрузки на бригады (людей);
- осуществляется проверка условия, если не удовлетворяет требованию, то осуществляется переход на начало алгоритма, если удовлетворяет условиям, то осуществляется вывод результатов;
- вывод результатов.

Данная методика позволяет определить численность, привлекаемого личного состава для контроля защищенности информации, необходимое количество средств и комплексов контроля защищенности информации на объектах информатизации.

Дубенецкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТЬЮ, ОРИЕНТИРОВАННАЯ НА ОБЪЕКТНУЮ МОДЕЛЬ ПРОЦЕССОВ

Проблемы внедрения и сопровождения ИТ-приложений для бизнеса:

1. Проблема разработки проекта внедрения и выбора прототипа информационной системы (ИС) для внедрения. Каждый проект внедренияпо своему оригинален и содержит большое число собственных прецедентов, объектов и событий.

2. Проблема сложности. Внедрение и сопровождение приложений требует существенных трудозатрат вследствие отсутствия электронной модели приложений и отсутствия встроенных высокоуровневых инструментальных средств настройки периода исполнения, разрыва между проектными решениями и кодом приложения.

3. Проблема управления процессами. Большинство приложений не обеспечивают адекватное описание и исполнение процессов, а предоставляют только набор сервисов для их поддержки. Управление процессами организуется на уровне внешних регламентов.

Требования к ИТ-приложениям для бизнеса**.** Ставится задача поиска такой модели бизнес-процессов, которая позволила бы обеспечить управление бизнес-процессами, направляя и контролируя действия пользователей и обеспечивая им доступ к необходимым сервисам ИС.

Деятельность, поддерживаемая приложением, должна быть описана в виде моделей процессов. Такая модель должна использоваться не только в виде функциональных требований в

ходе реализации, но и как основа исполнения любых операций пользователями в рамках своих обязанностей, синхронизации их работы, контроля исполнения и другое. Описания процессов должны позволить интегрировать все компоненты проекта ИС в единую систему в точном соответствии с требованиями Заказчика. Модель процессов должна быть интегрирована с остальными компонентами модели бизнеса. Модель бизнеса не должна «растворяться» в коде приложения, но должна быть встроена в приложение и использоваться им для решения задач управления.

Аналитические и расчетные компоненты должны быть относительно независимы и включаться в соответствующие состояния процессов при описании процессов.

Предлагаемые архитектурные решения. Технология расширения базовых каркасов приложения позволяет решить данные проблемы. Основу технологии составляет объектно-ориентированная модель приложения, реализованная в виде набора каркасов, которая может расширяться для решения проблем клиента с использованием специализированных инструментальных средств периода исполнения, Реализация расширений выполняется автоматически.

Инструменты формального описания бизнес-процессов, объектов и субъектов деятельности встраиваются в ИС. В ИС также включен открытый набор аналитических и расчетных программных модулей, позволяющий решать широкий спектр задач управления ресурсами.

Предлагается использовать технологию управления бизнес-процессами, которая позволяет строить формальные модели взаимодействующих процессов и делать их независимыми от функциональных программ.

Предлагаемая модель процессов тесно связана с моделью классов предметной области и является ее расширением. Конкретный процесс – это специальный класс, описание которого задает шаблон для создания и исполнения экземпляров процессов. Описание процесса разделено на две части. Первая часть содержит статическую модель процесса. Каждому процессу ставится в соответствие локальная модель классов, в которой заданы участники процесса (классы из локальной модели) и роли участников (ассоциации из локальной модели). Для каждого процесса могут быть указаны один или несколько основных классов-сущностей. Каждый класс из локальной модели содержит варианты поведения (процессы) для различных ролей.

Вторая часть содержит описание логики поведения экземпляров процесса и представляет процесс в виде автоматной модели (диаграммы состояний). Для каждого состояния определяются допустимые варианты поведения, указывающие доступные аналитические, расчетные и интерфейсные компоненты и их фактические параметры. Особое место в описании процессов занимают состояния, которые являются точками назначения объектов на роли и точками синхронизации экземпляров процессов. Сторожевые условия для состояний определяются как предикативные функции, заданные на множестве состояний процессов, допустимых решениях для состояний, предикатах, определенных на параметрах классов, включенных в локальную модель классов для процесса.

Таким образом, шаблон процесса задает все необходимые компоненты для создания и исполнения экземпляров процессов.

Предлагаемые решения прошли практическую апробацию при создании и внедрении системы ИС РЕСУРС.

Егупов М.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ЭЛЕКТРОННЫХ-ИНФОРМАЦИОННЫХ РЕСУРСОВ

Информационные технологии стали неотъемлемой частью современного общества. ЭВМ становятся не отъемлемым инструментом для решения многих задач. Мультимедийные приложения, многократно ускорили человеческую деятельность, а сетевые технологии объединили тысячи центров информации по всему миру. В значительной степени информационная революция повлияла и на образовательную сферу.

В настоящее время в объектах военного образования широкое распространение получили электронные учебники (ЭУ). Мною были рассмотрены ряд программ, позволяющие без специальных знаний и опыта осуществлять производство и редактирование электронных образовательных программ.

Прежде всего, обращаю внимание на то, что электронные учебники не должны быть альтернативным способом для подачи информации. Оптимальна ситуация, когда ЭУ расширяют возможности выбора для преподавателя при организации учебного процесса, не исключая использования технологий совместно с традиционными учебниками, а также живого общения. При этом ЭУ обладает рядом полезных качеств: высокая степень наглядности материала, взаимосвязь различных компонентов курсов, интерактивность, мультимедийность.

Рассмотрим несколько специальных программ для создания электронных учебников.

eBook Maestro. Универсальное средство создания электронных учебников. С помощью eBook Maestro можно вставлять в книгу ссылки на ресурс в Интернете, публиковать адрес электронной почты, а также создавать ярлыки. Можно задавать им свои названия на русском и английском языках. Все файлы книги, имеющей сложную структуру, хранятся в разных директориях.

Достоинства:

- поддержка HTML;
- обработка и сохранение данных, введённых пользователем в проект;
- преобразование текста в речь;
- быстрый и удобный поиск.

Недостатки: в бесплатной версии максимальное число файлов для одной книги – 500. То есть учебник будет ограничен количеством встроенных элементов. В платной версии количество знаков не ограниченно.

ChmBookCreator – это средство, способное из разнородных файлов htm, txt, doc и rtf создавать электронное пособие, внешне похожее на обычную книгу.

Достоинства:

- есть возможность создавать собственный уникальный дизайн для пособия;
- удобен для неопытного пользователя;
- наличие подробной встроенной справки.

Недостатки:

- в CHM файлах нет закладок.
- медленная обработка файлов.

Learning Content Development System. Система управления обучением

Система предназначена для создания электронных учебников с интерактивными тестами, демонстрационными роликами, экзаменами и анимацией. Использование среды не требуется никаких особых навыков программирования или дизайна. Интерактивные курсы строятся путем создания и настройки различных модулей на основе готовых шаблонов с использованием созданных автором аудио и видео клипов и других мультимедийных файлов.

Достоинства:

- создание веб-материалов, соответствующих набору стандартов Sharable Content Object Reference Model (SCORM) и пригодных к использованию в системах для управления обучением.
- выбор форм из широкого многообразия форм для создания эффективных электронных курсов и интерактивных компонентов на основе технологии Silverlight.

Также к неоспоримым преимуществам программы Learning Content Development System является поддержка технологии Windows Presentation Foundation (WPF).

Недостатки: необходимость установки плагинов для корректного отображения учебных материалов.

В целом, при выборе средств разработки электронных учебников необходима оценка наличия:

- аппаратных средств определенной конфигурации;
- сертифицированных программных систем.

Информация взята с сайтов-разработчиков описанных программных средств, а также сформирована на основе личной эксплуатации пробных версий описанных программ.

Жук А.А., Климов А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПЛАНИРОВАНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Поиск путей сокращения длительности цикла планирования и управления остаётся одним из важнейших направлений в оптимизации управления. В условиях скоротечности современного боя время на принятие решения лицом, принимающее решение, должно быть минимально возможным. Выработанное решение должно быть обоснованным, опираться на необходимые расчеты и содержать информацию, которая может быть представлена в текстовом и графическом виде.

Сокращения времени на принятие решения и его обоснованность явились предпосылками необходимости автоматизации управления. Постоянная готовность автоматизированных систем управления к использованию по назначению и эффективность их применения достигается правильной организацией технического обслуживания и его планированием.

Как и большинство реальных задач, задача планирования технического обслуживания строится на основе вероятностной сетевой модели.

Исходные данные могут представляться в табличном виде: номера и наименование работ, номера предшествующих работ и время выполнения (мин. и макс.)

Результат решения представляет сетевой граф, параметры сетевого графа и критического пути. По полученному сетевому графу строиться сетевой план. Как правило исходный сетевой план

не удовлетворяет требованиям и требует улучшения. Улучшение сетевого плана производиться по времени и использования людских и материальных ресурсов. Оптимизация по времени предполагает либо поиск сетевого графа с минимальной длиной критического пути, либо с длиной, не превышающей заданную. Оптимизация по ресурсам предполагает поиск сетевого плана с равномерным использованием ресурсов на протяжении всего технического обслуживания. Несмотря на то, что существует ряд формальных методов оптимизации сетевого плана, практически все известные программные продукты сетевого планирования реализованы на основе метода последовательного приближения. Это объясняется тем, что всегда имеют место неформальные признаки или элементы ИД, которые явно не учитываются.

Сетевой план обычно представляется в виде диаграмм Гантта для работ и распределения ресурсов.

Улучшение сетевого плана производиться по алгоритму:

- анализ сетевого плана и определение возможных направлений улучшений улучшения;
- внесение улучшений и расчет параметров сетевого графа;
- проверка выполнения требований;

Данный процесс повторяется до получения положительного результата проверки или пока не будут исчерпаны все возможности улучшения сетевого плана.

Готовый сетевой план привязывается к календарному графику.

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ТРАНСПОРТОМ В МЕГАПОЛИСЕ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА

Практика организации управления жизнедеятельностью современных мегаполисов показывает, что эффективность данного процесса во многом определяется наличием и качеством информационных систем управления, а также принципами их совместного использования в процессе управления.

Среди имеющегося разнообразия подходов к построению систем управления мегаполисом, особенно в условиях практического использования уже развернутых систем автоматизированного управления различными отраслями его жизнедеятельности, построение единой су жизнедеятельностью является сложной многокритериальной задачей. На сегодняшний день не существует единой методики, предписывающей обоснованный выбор соответствующей конкретным условиям жизнедеятельности системы управления. В докладе рассматриваются особенности построения современных систем управления транспортом, а также существующие подходы для организации управления отдельными областями жизнедеятельности крупных мегаполисов (безопасностью жизнедеятельности (КСОБЖН), обеспечением правопорядка (АПК «БГ»)) и предлагается решение по построению архитектуры СУ мегаполисом по примеру архитектуры системы «Smart Sity».

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ МЕГАПОЛИСОМ - «SMART SITY»

В настоящее время в мире большую популярность приобрела идея построения «умной» системы управления мегаполисами (системы «Smart Sity»). Вместе с тем, четкого единого понимания о функциональном и структурном составе данной системы пока нет. Каждый вкладывает свой смысл в данное понятие, т.к. это обычно зависит от статьи бюджета Заказчика. Отсутствие чёткой идеологии, желание придать любому решению статус «умной» технологии для города, приводит к тому, что чаще всего под «умным» подразумевают лишь систему Безопасный город, иногда к нему еще добавляются системы ОБЖД и управления транспортом.

Среди имеющегося разнообразия подходов к построению систем управления мегаполисом, особенно в условиях практического использования уже развернутых систем автоматизированного управления различными отраслями его жизнедеятельности, построение единой су жизнедеятельностью является сложной многокритериальной задачей. На сегодняшний день не существует единой методики, предписывающей обоснованный выбор соответствующей конкретным условиям жизнедеятельности системы управления.

В мировой практике, в целом, под «Smart Sity» понимают реализацию комплекса решений по следующим направлениям:

- решения, ориентированные на «зеленые» технологии, основным посылом которых является снижение выбросов CO2 и использование возобновляемых источников электроэнергии;
- решения, обеспечивающие транспортную безопасность и эффективное управление транспортными потоками;

– решения, обеспечивающие охрану правопорядка и безопасность жизнедеятельности населения;

– решения, направленные на накопление и перераспределение энергии (Smart-grid);

– решения, направленные на раздельный сбор и переработку ТБО;

– системы городского информирования eTurist;

Чаще всего на практике, под современными решениями типа «Smart Sity» понимают одно из выше перечисленных направлений или, в лучшем случае, комбинацию из 2 или 3 направлений.

УМНЫЙ ГОРОД – это «… комплекс программно-технических решений и организационных мероприятий, направленных на создание высокотехнологичной наукоемкой экономики, эффективное использование всех видов ресурсов (электричество, вода, газ/тепло, пространство, время), устойчивое социально-экономическое развитие города и создающих условия для удобного пребывания в городе, комфортного проживания и ведения бизнеса …».

Предлагаемые и реализуемые за рубежом и в России стратегии, концепции, подходы, модели и проекты по созданию Умных городов, можно свести к общей модели, включающей семь составляющих:

– умная экономика (smart economy);

– энергоэффективность и ресурсосбережение (smart energy);

– умная среда обитания (smart environment);

– мобильность (smart mobility);

– умное население (smart people);

– умное управление (smart governance);

– комфортность проживания (smart living).

«Умный Город» для городских властей это:

– Обеспечение мер безопасности и эффективное управление деятельностью экстренных и оперативных служб;

– Мониторинг и управление угрозами и чрезвычайными ситуациями, влияющими на среду обитания (защита населения и городского хозяйства от угроз: террористических, криминальных и экстремистских, природных, техногенных (в сфере энергетики, транспорта и ЖКХ и пр.), экологических, биологических и др.);

– Переработка и утилизация отходов производства и потребления (мусора), раздельный сбор мусора.

– Очистка сточных вод, управление ливневыми стоками.

– Энергоэффективность и ресурсосбережение – использование энергосберегающих, экологичных и безопасных технологий и решений в топливно-энергетическом комплексе (включая водоснабжение), ЖКХ, градостроительстве и на транспорте. Комфортное жильё, Умный дом/здание.

– Система городского оперативного оповещения

– Многофункциональные центры (МФЦ), обслуживающие жителей и организации по принципу «одного окна», государственные и муниципальные услуги, а также дополнительные информационные, заказывающие и платежные сервисы в электронном виде (через Интернет-порталы, мобильные приложения, информационные киоски, терминалы) в сфере ЖКХ, связи, транспорта, торговли, быта, банковского обслуживания, налогов, страхования, культуры, спорта, отдыха, туризма и пр;

– Городское видеонаблюдение для предотвращения правонарушений;

– Система фиксации нарушений ПДД и сбора штрафов;

– Планирование расходов на оплату коммунальных услуг бюджетных организаций;

– Удобный общественный транспорт, транспортная доступность, снижение загруженности УДС Отслеживание «пробок» и управление дорожным движением;

– Градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма и промышленной архитектуры индустриальных парков и их совместимости.

– Экологический и биологический мониторинг окружающей среды (атмосфера, гидросфера, почва, биосфера), использование возобновляемых источников энергии (солнечные, ветряные, геотермальные, приливные, биотопливные);

– GPS/GLONASS мониторинг городского транспорта и транспорта экстренных служб;

– Обслуживание общегородской инфраструктуры;

– Прозрачное предоставление образовательных услуг (электронное образование (электронные библиотеки, учебники, дневники, журналы, портфолио, мультимедийные презентации, интерактивные доски, дистанционное обучение для лиц с ограниченными возможностями, системы ВКС и телеприсутствия, системы управленческого учета в учебных заведениях));

– Прозрачное предоставление медицинских услуг (электронная и телемедицина (электронные медицинские карты, дистанционное обследование и консультации, электронный рецепт,

круглосуточное дистанционное наблюдение и лечение, системы ВКС и телеприсутствия, МИС и системы управленческого учета в ЛПУ));

– Информационно-картографическое обеспечение и т.п.

«Умный Город» для жителей это:

• Система самообслуживания через личный кабинет для оплаты услуг ЖКХ;

– Решения по экономному расходованию всех видов коммунальных ресурсов;

– Быстрое предоставление государственных услуг городскими властями;

– Карта жителя города (ID, проезд в городском транспорте, система предоставления скидок, оплата за товары и услуги);

– Внутридомовое (входы в здания, лифты, этажные площадки...) и наружное видеонаблюдение;

– Электронная запись для получения бытовых или медицинских услуг;

– Системы погодно-климатического и экологического мониторинга;

– Парковочный информатор;

– Электронное расписание (графики работы и обслуживания, транспорт)

– Интеллектуальная транспортная система (транспортная доступность в частности).

– Градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма (пешеходная доступность в частности).

– Скоростная ИКТ-инфраструктура (проводная и беспроводная).

– M2M-технологии/Интернет вещей (Internet of Everything – IoF)/ Всеобъемлющий Интернет (Internet of Things – IoT).

– Публичные и социальные сервисы на базе открытых интернет-порталов (Web-приложений) и мобильных приложений.

– Высокотехнологичные многофункциональные персональные ИКТ-устройства (связь, определение местоположения, удаленный доступ к ресурсам и услугам, контроль, диагностика, регистрация, управление, оповещение).

– Системы видеоконференцсвязи (ВКС) и телеприсутствия.

– Мобильные, информационные и платежные сервисы, электронные пластиковые карты (ID, различные виды платежей, безопасность, банковские, транспортные и др. виды услуг).

«Умный Город» для Управляющих и ресурсо-снабжающих компаний это:

– Система автоматизированного сбора данных с приборов учета и мониторинга оборудования инженерных систем, находящихся на обслуживании;

– Система автоматизированного управления инженерными системами, находящимися на обслуживании;

– Своевременное выставление счетов и контроль оплат;

– Решения по экономному расходованию всех видов коммунальных ресурсов;

– Формирование и выдача ТУ для тех. присоединения новых клиентов;

– Отчеты в режиме реального времени по потреблению всех видов ресурсов, как в масштабе города, так и в более мелкой детализации (квартал, здание, квартира, организация и т.п.)

– Краткосрочные и долгосрочные прогнозы по потреблению ресурсов;

– Видео-мониторинг за подотчётной территорией;

– Обеспечение автоматического и диспетчерского отключения систем при наступлении природных или техногенных катастроф;

– План проведения регламентного обслуживания сетей и зданий;

– Погодно-ориентированное поведение инженерных систем;

– Отчетность для органов местного самоуправления.

Проблемы реализации:

– Отсутствие единого собственника, ведомственная разобщенность;

– Зависимость от местных властей в интеллектуализации общегородской инфраструктуры;

– Нет статистики по реальной окупаемости «умных» технологий;

– Нет поддержки со стороны государства энергоэффективных решений;

– Отсутствует добрая воля для предоставления открытых данных для сторонних разработчиков и всех желающих;

– Все еще не высокая компьютерная грамотность населения

Журавель Е.П.
Россия, Санкт-Петербург, АО «НИИ «Рубин»

МОДЕЛИ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Предоставление услуг связи осуществляется с использованием ресурсов мультисервисной сети связи (МССС), представляющих собой совокупность элементов активной и пассивной сетевой инфраструктуры, физических или логических компонентов (микропрограммного обеспечения) телекоммуникационного оборудования (ТКО), средств вычислительной техники (СВТ) и соответствующих видов общего, специального и другого программного обеспечения, используемых для формирования услуг электрической связи, совместная эксплуатация которых направлена на удовлетворение потребностей пользователей МССС в традиционных и перспективных услугах электрической связи. Множество услуг МССС совокупностью своих характеристик определяет необходимые перечень и значения функциональных требований к свойствам ресурсов МССС. В свою очередь, обладающие конечной пропускной способностью и производительностью ресурсы МССС определяют нагрузочные ограничения по количеству и/или качеству предоставляемых услуг МССС.

В соответствии с рекомендациями международного форума по построению и развитию сетей пакетной передачи информации и предоставляемых ими услугах (http://broadband-forum.org),применительно к МССС, ее ресурсы целесообразно рассмотреть, учитывая особенности обработки данных, устойчивость и безопасность предоставления услуг, для чего целесообразно выделить следующие сети МССС, ее составляющие:

- сети доступа - часть МССС, которая связывает источник (приёмник) сообщений абонента с ТКО узла доступа пункта присутствия оператора связи;
- сети агрегации - часть МССС, выделяемая как отдельная сеть в крупных и/или территориально распределенных сетях, агрегирующая данные от многочисленных узлов доступа пункта присутствия оператора связи для их передачи по небольшому числу высокоскоростных каналов связи до ТКО, являющегося граничным между сетью агрегации и транспортной сетью;
- транспортные сети - часть МССС, выполняющая функции переноса (транспортирования) потоков сообщений от их источников из одной сети доступа (возможно, с использованием её сети агрегации) к получателям сообщений другой сети доступа (возможно, с использованием другой сети агрегации);
- сети систем коммутации - часть МССС, соединенная с транспортной сетью или с сетью агрегации и выполняющая функции формирования, предоставления и учета предоставления услуг связи и, возможно, дополнительных видов обслуживания с требуемым качеством, а также мониторинга качества их предоставления с использованием, в том числе, механизмов аутентификации, авторизации и, возможно, аккаунтинга с последующим формированием данных предбиллинга;
- сети управления - часть МССС, являющаяся основой для кроссплатформенной системы управления ТКО МССС с использованием принципов автоматизированного конфигурирования сетевых устройств и протоколов безопасного сетевого соединения, в том числе используемая для решения задач резервного копирования конфигураций ТКО и автоматизации отслеживания изменений в конфигурации ТКО;
- сети обеспечения функционирования - часть МССС, реализующая функции обеспечения синхронизации точного времени, функции именования сетевых элементов на основе единого указателя ресурсов с использованием системы доменных имён, сетевой идентификации и/или аутентификации, авторизации, аккаунтинга и учёта использования услуг с объединением их в иерархию с целью формирования услуги "Удостоверение как услуга" для технических специалистов организации связи и/или программного обеспечения автоматизированных систем управления ТКО и/или СВТ.

С учетом рассмотренных выше особенностей построения сетей, составляющих МССС, целесообразно выделить следующие основные модели ресурсов МССС:

- модели характеристик ресурсов МССС;
- модель точки присутствия (ТП) ресурсов МССС;
- модели ТКО и СВТ оператора связи, размещенные в ТП МССС;
- модели линейно-технических элементов сетевой инфраструктуры (ЛТЭСИ) МССС;
- модели связей ЛТЭСИ и ТКО и СВТ МССС;
- модели связей ТКО и СВТ и услуг МССС.

Рассматриваемые модели ресурсов МССС позволяют получить формальное описание задачи учета и предоставления услуг МССС с использованием ее ресурсов, имеют однозначный физический смысл, облегчают обнаружение возможных ошибок и несоответствий, обладают достаточной общностью и в совокупности учитывают функциональные и нагрузочные требования к количеству и к качеству предоставляемых МССС услуг.

Журавель Е.П.
Россия, Санкт-Петербург, АО «НИИ «Рубин»

МОДЕЛИ УСЛУГ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Основным видом телекоммуникационной сети связи единой сети электрической связи (ЕСЭС) Российской Федерации (РФ) является мультисервисная сеть связи (МССС) с использованием преимущественно пакетных методов передачи информации (данных, сообщений), представляющая собой совокупность телекоммуникационных и информационных ресурсов, совместная эксплуатация которых направлена на удовлетворение потребностей пользователей в традиционных и перспективных услугах электрической связи.

Рассмотрение процессов предоставления услуг ресурсами МССС целесообразно осуществлять на основе обобщённой модели предоставления услуг, под которой, в соответствии с рекомендациями международного форума по построению и развитию сетей пакетной передачи информации и предоставляемых ими услугах (http://broadband-forum.org), понимается предоставление услуг электрической связи с заданным (требуемым) качеством посредством использования различных технологий, протоколов и сред передачи информации на любом порту абонентского оконечного устройства, если порт способен предоставлять данную услугу, любым выбираемым пользователем оператором связи, таких, например, как:

- услуга передачи информации, характеризующаяся отсутствием жёстких требований к процессу передачи (допускается произвольное многократное изменение скорости передачи в процессе передачи, возможны потери, переприёмы, обрывы соединения и восстановление процесса передачи как с учётом информации состояния, так и без него и пр.);
- услуга передачи сообщений, являющаяся частным случаем услуги передачи информации и в общем случае характеризующаяся отсутствием требований к необходимости непосредственной одновременной готовности источника и приёмника сообщений (сообщения электронной почты и др.);
- услуга передачи видеоинформации, налагающая существенные требования по пропускной способности в единицу времени, порядку следования пакетов, отсутствию потерь и видам трафика передаваемой информации;
- услуга передачи голосовой информации, налагающая жёсткие требования к процессу и минимальной пропускной способности среды передачи информации, а также отсутствию случайных задержек распространения и потерь пакетов при передаче;
- услуга управления активным телекоммуникационным оборудованием (ТКО) и средствами вычислительной техники, составляющими ресурсы МССС, также характеризующаяся жёсткими требованиями к отсутствию потерь пакетов и к достоверности передаваемой информации.

Анализ процессов предоставления услуг МССС позволяет утверждать, что, как правило, достаточно полно известны только основные количественные значения параметров услуг, характеризующие их предоставление.

Оценка интенсивности предоставления услуг МССС с коммутацией пактов на основе анализа протекающих в ней процессов заключается в анализе процессов предоставления услуг пользователям МССС и формулировании выводов о стационарности, ординарности, непрерывности и последействии входного потока запросов на предоставление услуг, основными из которых являются:

- процесс предоставления услуг МССС в общем случае не может рассматриваться как стационарный, что обусловлено отсутствием регламентации деятельности пользователей МССС и, как следствие, нерегулярностью порождения запросов на получение услуг МССС;
- неординарность предоставления услуг МССС обусловлена отличной от нуля вероятностью возникновения нескольких заявок на предоставление двух и более услуг в один и тот же момент времени, а в случае одновременного возникновения нескольких заявок на предоставление услуг соответствующая телематическая служба МССС осуществит их обработку последовательно в порядке появления их в своей очереди;
- последействие обусловлено зависимостью некоторых услуг МССС от других услуг, что, в свою очередь, при предоставлении услуги одного типа может вызвать "всплеск" интенсивности запросов на предоставление услуг другого типа, порожденных данной услугой, а для некоторых услуг последействие присуще изначально ввиду наличия у человека как пользователя МССС известного в инженерной психологии эффекта, заключающегося в том, что человек запоминает и стремится полностью завершить начатое и не законченное им действие.

Предлагаемые модели услуг МССС обладают достаточной общностью, адекватностью и достоверностью, не зависят от технологий и/или сред передачи, необходимых для их предоставления и позволяют осуществить моделирование услуг для соответствующих технологий и/или протоколов и/или сред передачи, обладающих требуемой для предоставления услуг пропускной способностью и характеризующихся совокупностью значений соответствующих параметров.

Журавель Е.П., Журавель П.Н., Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «НИИ «Рубин», АО «РАМЭК-ВС», АО «Институт инфотелекоммуникаций»

МОДЕЛИ ВОЗДЕЙСТВИЙ НА РЕСУРСЫ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Основными характеристиками единой сети электрической связи (ЕСЭС) Российской Федерации являются целостность, устойчивость и безопасность её функционирования, соответственно, указанными характеристиками должны обладать и сети ЕСЭС, её составляющие. Модели источников угроз (нарушителей), угроз, деструктивных воздействий, технологий и (или) сред передачи деструктивных воздействий, а также ресурсов применительно к МССС целесообразно рассмотреть с учётом особенностей построения и функционирования МССС.

Перечень соответствий объектов доступа и ресурсов МССС, на которые могут оказывать воздействие источники угроз, представляет собой произвольное множество, изменяющееся во времени, поскольку виды угроз и источников угроз, а также виды обеспечения и ресурсы МССС потенциально динамичны и расширяемы на соответствующих стадиях и процессах жизненного цикла МССС. В целом, исходя из анализа модели источников угроз МССС, учитывая объективные и субъективные классификационные признаки источников угроз, можно сделать вывод о том, что их выявление и (или) полное устранение не представляется возможным и формируемые ими угрозы необходимо учитывать на всех этапах жизненного цикла МССС. Также следует отметить, что выявление и построение полного множества угроз безопасности МССС не поддаётся формализации.

Модель технологий и (или) сред передачи деструктивных воздействий на ресурсы МССС, целесообразно формировать на основе эталонной модели взаимодействия открытых систем (ЭМВОС) и функциональных классификационных признаков подсетей МССС, её составляющих. С учётом определяющей роли информации применительно к МССС, целесообразно рассмотрение возможных угроз безопасности на соответствующих уровнях ЭМВОС. Модель технологий и (или) сред передачи деструктивных воздействий на ресурсы МССС, при всем существующем многообразии возможных вариантов, всё-таки характеризуется свойством конечности, что обусловлено ограниченным и достаточно не большим количеством непрерывно совершенствуемых современных телекоммуникационных технологий и протоколов, их реализующих, а также использованием открытых спецификаций и исходного кода, разрабатываемых международным сообществом с учётом требований по обеспечению безопасности и всесторонним контролем их выполнения.

Модели ресурсов МССС, требующих защиты, в общем случае включают в себя телекоммуникационное оборудование (ТКО) и средства вычислительной техники (СВТ), их организационное, методическое, математическое, лингвистическое, эргономическое, информационное и программное обеспечение.

По классификационному признаку вида воздействия на ресурсы МССС целесообразно выделить следующие модели воздействий на ресурсы МССС:

- модели деструктивных технических воздействий на ресурсы МССС, представляющие собой физические воздействия на элементы МССС, организационно-технические приёмы и способы защиты от которых в достаточной мере проработаны;
- модели деструктивных программных воздействий на МССС также известны и, в свою очередь, могут быть классифицированы по классификационному признаку возможности распространения на локальные и получившие в настоящее время наибольшее распространение сетевые, а также по характеру воздействия на программное обеспечение ТКО и автоматизированных систем управления таким оборудованием (уничтожение, повреждение, модификация и пр.), способы защиты от которых проработаны и получили реализацию в достаточном количестве антивирусных и других программных средств;
- модели деструктивных программно-технических воздействий на ресурсы МССС введены на основе результатов анализа специальных воздействий на техническое обеспечение ТКО сети связи, к которым, можно, например, отнести случайное программное обращение на чтение к секторам накопителя на жестком магнитном диске (НЖМД) СВТ или ТКО, причем настолько часто и настолько быстро, насколько НЖМД на это способен. Результатом будет являться перегрев НЖМД, возможно, с одновременной разъюстировкой головок чтения-записи дисковых НЖМД или сокращением и/или исчерпанием ресурса чтения-записи секторов НЖМД на основе твердотельных носителей информации и, как следствие, отказ НЖМД и, в связи с этим, отказ СВТ или ТКО.

Ввиду непрерывно и динамически изменяющихся условий применения и функционирования МССС, полная априорная и достоверная количественная оценка значений параметров воздействий на ресурсы МССС не представляется возможной и для её получения целесообразно использовать требования соответствующих руководящих документов, определяющих цели и задачи применения МССС по предназначению. Для своевременного выявления и непосредственной оценки воздействий с целью принятия необходимых мер защиты и их уточнения, следует осуществлять необходимый и достаточный по полноте и периодичности сбор информации состояния значений параметров функционирования ресурсов МССС.

Зайцев Ф.С., Кузнецов Д.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ВОЗМОЖНОСТИ ПОМЕХОУСТОЙЧИВЫХ КОДОВ ПО ПОВЫШЕНИЮ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ

С ростом возможностей цифровой обработки информации при использовании высокопроизводительных процессоров все более актуальным становится вопрос энергетической эффективности.

Поскольку помехоустойчивое кодирование позволяет исправлять ошибки, при его применении можно оставляя скорость передачи информации неизменной снизить мощность передатчика, уменьшить величину и сложность антенны или увеличить дальность связи. На сегодняшний день в теории кодирования известно много кодов и методов их декодирования, различающихся энергетическим выигрышем, вносимой избыточностью, сложностью реализации и рядом других параметров.

Наиболее популярным методом коррекции ошибок в последнем десятилетии является применяемый для декодирования сверточных кодов декодер Витерби. Он используется в беспроводных сетях IEEE 802.11, IEEE 802.16, дальней космической связи CCSDS, спутниковой связи TIA-1008. Данный алгоритм достаточно легко реализуется для коротких сверточных кодов, однако с ростом длинны кода сложность его реализации растет в геометрической прогрессии.

Следующим этапом развития методов коррекции ошибок для декодирования сверточных кодов с большей длинной стали последовательные алгоритмы декодирования. С точки зрения теории помехоустойчивого кодирования последовательные алгоритмы декодирования работоспособны только в области, меньшей чем вычислительная скорость канала.

Появление каскадных кодов, в основе которых лежит идея совместного использования нескольких различных кодов, стало одним из основных вех в развитии теории помехоустойчивого кодирования. Каскадный код позволяет с помощью декодеров относительно простых составляющих кодов эффективно декодировать всю кодовую конструкцию. Для примера в современных системах передачи данных (CCSDS, DVB-H/T/S, IEEE 802.16, TIA-1008) применяется каскадная схема, в которой данные сначала кодируются внешним кодом Рида-Соломона (RS), а затем внутренним сверточным кодом, декодируемым с помощью декодера Витерби.

Для декодирования очень длинных кодов (с линейной сложностью реализации, зависящей от длинны кода) используется более эффективный многопороговый декодер (МПД) самоортогональных кодов который является развитием простейшего порогового декодера Месси.

Потенциальные возможности МПД позволяют принять его как один из основных методов коррекции ошибок для многих современных высокоскоростных систем передачи данных с предельно возможными уровнями энергетического выигрыша и быстродействием, достигающим сотен и тысяч Мбит/с.

Практически параллельно с развитием каскадных кодов шло исследование турбо кодов, образующихся путем каскадирования двух или более составляющих кодов. В общем случае турбо коды могут получаться как при параллельном, так и последовательном соединении кодов, разделенных перемежителем.

Экспериментально выяснено, что для параллельного турбо кода наилучшими составляющими являются рекурсивные систематические сверточные коды. Получающийся в результате турбо код обычно называется сверточным турбо кодом (Turbo Convolutional Code – TCC).

На сегодняшний день различные варианты турбо-кодов рекомендованы к применению и используются в таких стандартах беспроводной связи, как CCSDS, TIA-1008, CDMA2000, UMTS.

Основными недостатками TCC, мешающими его продвижению является относительно сложная практическая реализация, а также наличие области насыщения вероятности ошибки.

Для борьбы с эффектом насыщения вероятности ошибки используются двойные турбо коды (рекомендованных в стандартах DVB-S, IEEE 802.16).

Для последовательного каскадирования двух и более блоковых кодов используются турбо коды произведения (Turbo Product Code – TPC). Для TPC применим итеративный алгоритм декодирования, позволяющий при невысокой сложности реализации получать близкую к предельной эффективность декодирования.

Системы передачи данных, использующие TPC способны работать при очень низких отношениях сигнал/шум и показывают хорошую адаптивность к предъявляемым требованиям по корректирующей способности, вносимой избыточности, длинам используемых кодов и др. Коды TPC используются во многих системах передачи данных, таких как INTELSAT, IEEE 802.16.

Существует еще отдельный класс кодов, рекомендуемых для исправления ошибок в новых стандартах передачи различного рода данных (DVB-S2, 802.11n, 802.16e)-это низкоплотностные коды. Коды с малой плотностью проверок на четность (Low-Density Parity-Check – LDPC) при

применении методов итеративного декодирования позволяет практически вплотную приблизиться к пропускной способности канала при относительно небольшой сложности реализации.

LDPC коды представляют собой линейные блоковые коды, задаваемые с помощью проверочной матрицы H, характеризуемой относительно малым (<10) числом единиц в строках и столбцах.

На сегодняшний день существует всего несколько методов коррекции ошибок, способных работать вблизи пропускной способности канала.

Это многопороговые декодеры самоортогональных кодов, турбо и низкоплотностные коды. Каждый из них имеет свои достоинства, недостатки и, соответственно, свою область применения.

Например, турбо и низкоплотностные коды, способные работать при уровне энергетики канала, всего на несколько десятых децибела превышающих его пропускную способность требуют для практической реализации значительные аппаратные ресурсы. В результате разработчики или используют чрезвычайно дорогие аппаратные средства, или идут на упрощение алгоритмов, что приводит к ухудшению характеристик. Многопороговые декодеры, хотя и уступают турбо и низкоплотностным кодам по обеспечиваемому уровню энергетического выигрыша, позволяют создавать недорогие кодеки МПД, успешно работающие в высокоскоростных цифровых системах передачи данных за счет простой реализации.

Зорин К.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНТЕГРАЦИЯ ДАННЫХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ ДЛЯ ПОЛУЧЕНИЯ НОВОЙ ИНФОРМАЦИИ

Программный продукт или информационная система, с которыми взаимодействуют пользователи, или даже деятельность какого-то предприятия в целом, представляют собой сложную систему, которая не может быть наблюдаема напрямую и целиком.

Для наблюдения и анализа система доступна только в некоторых проекциях. Каждый источник данных, имеющий отношение к системе и содержащий данные определённой тематики, представляет из себя такую проекцию.

На примере предприятия, ведущего бизнес в сфере информационных технологий, такими источниками данных являются:

- корпоративные информационные системы, включающие системы учёта продаж, планирования ресурсов;
- системы мониторинга корпоративных информационных ресурсов (информация о посещении сайтов и т.д.);
- системы интернет-маркетинга, системы управления емейл-рассылками и коммуникациями с клиентами;
- системы службы поддержки, системы учёта дефектов и ошибок (баг-трекеры);
- данные из социальных сетей.

Но чтобы иметь картину в целом, необходимо консолидировать источники данных, иинтегрировать данные из них. Интеграция данных из этих систем даёт системный эффект — новую информацию, которой не было ни в одной системе по отдельности.

В настоящее время для подобных задач используется концепция Data Lake («Озеро данных») — общее хранилище данных, куда «ручейками» и «реками» стекаются данные из различных источников. Особенностью этой концепции является то, что данные попадают из разнородных хранилищ не только для структурированной информации, но и для слабоструктурированной или даже для неструктурированной информации. Для этого применяются как классические реляционные СУБД, так и нереляционные масштабируемые и распределённые NoSQL-решения.

Иванов В.Г., Башлаев Р.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ТРЁХМЕРНЫХ ОБЪЕКТОВ ДЛЯ УВЕЛИЧЕНИЯ ИНФОРМАТИВНОСТИ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО (СПЕЦИАЛЬНОГО) НАЗНАЧЕНИЯ

Потребность подробного изучения местности была всегда актуальна для военных пользователей. Исторически, информация о местности, как на стратегическом, так и на тактическом уровнях представлялась бумажными картами. В связи с чем одной из основных задач топогеодезического обеспечения является актуализация карт и своевременное обеспечение войск достоверной топографической информацией, представление которой в аналоговом виде имеет ряд недостатков.

Одно из основных требований к картам военного назначения – отражение достоверной, актуальной информации о ситуации в ходе боевых действий. Карта представляет собой единую структуру, на которую накладывается оперативно-тактическая обстановка, отражающая текущий

баланс сил и их рассредоточение на местности. Основными недостатками аналоговых карт являются: продолжительное время необходимое для обновления оперативно-тактической обстановки и трудности в своевременном доведении актуальной информации до конечных пользователей.

С появлением современных компьютерных технологий, на смену аналоговым картам пришли цифровые геоинформационные системы. Благодаря повсеместной информатизации войск, использование геоинформационных систем стало доступно на всех этапах планирования и проведения операций. Введение геоинформационных систем позволило сократить время на актуализацию обстановки и принятие решения командирами на «цифровом поле боя». Процесс актуализации информации происходит по различным каналам, что позволяет командирам получать информацию об изменении тактической обстановки в кратчайшие сроки.

На данный момент большинство геоинформационных систем работает с двумерными картами и объектами. В свою очередь геоинформационная система, работающая с двумерными объектами и картами, не способна в полной мере передать всю пространственную информацию по интересующему району.

В связи с чем для увеличения информативности геоинформационной системы вводится трехмерное отображение топогеодезических данных и оперативно-тактической обстановки. Трехмерное представление местности позволяет командиру более детально изучить район операции, что в свою очередь сокращает время на принятие решения и позволяет качественнее прорабатывать операции с учетом объектов поля боя и рельефа местности.

Применение трехмерного моделирования позволяет наилучшим образом отразить актуальную оперативно-тактическую обстановку на местности, объекты окружающего мира и их взаимное расположение, используя технологию построения трехмерных моделей. Технология построения трехмерной модели реализована на базе приложений, входящих в состав геоинформационной системы специального назначения «Оператор».

Данные средства позволяют создавать трехмерные модели местности, архитектурных сооружений, техники, живой силы, интерьера помещений, надземных и подземных коммуникаций, а также моделировать перемещения объектов на местности.

Одной из основных задач по созданию трехмерной карты оперативно-тактической обстановки театра боевых действий является разработка библиотеки трехмерных объектов, которые будут соответствовать требованиям, предъявляемым к отработки картографических документов.

В дальнейшем трехмерные карты тактической обстановки могут использоваться для решения как учебных, так и боевых оперативно-тактических задач проведения учений и военных игр.

Иванов В.Г., Полячков А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБРАБОТКА СЛАБОСТРУКТУРИРОВАННЫХ ДОКУМЕНТОВ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В СОСТАВЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Развитие современной армии, как и развитие современного общества в целом, базируется на внедрении и развитии информационных технологий. К подобным технологиям можно отнести системы поддержки принятия решений (далее СППР), использующие в своем составе геоинформационные системы (далее ГИС). Составной частью подобных систем является средства обработки цифровой информации о местности во взаимосвязи с многообразными данными о противнике и своих войсках.

Подобные системы поддержки принятия решений используют в качестве источника входной информации текстовые документы. Они импортируют информацию в текстовой форме, классифицируют её по рубрикам для последующего анализа в соответствии с иерархией рубрик для дальнейшего использования. Во многих случаях текстовый документ получается из речевого сообщения после обработки средствами распознавания речи.

Качество анализа документов определяется не только совершенством систем ввода, анализа, но и типом самого документа. В зависимости от структуры, документы можно разделить на следующие типы: структурированные, слабоструктурированные, неструктурированные.

В СППР военного применения, работающими с ГИС чаще всего используются слабоструктурированные и неструктурированные документы, анализ которых принято относить к сложным задачам, решение которых требует привлечения определенных средств и занимает время, которого в реальных условиях всегда недостаточно.

Большинство известных нам методов анализа текстов, так или иначе, основаны на предположении, что тексты каждой тематической рубрики содержат отличительные признаки (слова или словосочетания) и наличие или отсутствие таких признаков в тексте говорит о принадлежности или непринадлежности исследуемого текста той или иной рубрике

Известны следующие автоматические методы анализа текстов: статистические, частотные, шаблонные, на основе нейронных и семантических сетей, основанные на деревьях.

Очень часто применяется, как классический метод, для понимания текста частотный анализ. Этот метод относится к наиболее быстродействующим и не требует выделения большой емкости памяти и вычислительных ресурсов.

Сущностью частотного анализа является определение частоты появления ключевых слов в тексте. По частоте появления можно определить предметную область текста. Ограничением частотного метода является то, что он не дает хороших результатов для текстов малых размеров, и поэтому для них не применяется. В рассматриваемой же тематике в качестве обрабатываемых документов и используются короткие текстовые документы. Однако частотный метод применим и для коротких текстов и даже их фрагментов. Для классификации таких текстов необходимо анализировать дополнительные параметры и особым образом их обрабатывать.

К дополнительным параметрам можно отнести, например: положение ключевых слов в тексте, расстояние между ключевыми словами, наличие специальных символов.

Использование улучшенного алгоритма для автоматизация процесса обработки входных документов позволит существенно повысить оперативность работы СППР работающей с ГИС за счет более эффективного использование привлекаемых для работы средств и сократить время на принятие решений.

Иванов М.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОПЫТ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ SDR ПРИ ДЕКОДИРОВАНИИ СИГНАЛОВ СТАНДАРТА IEEE802.11G

Постоянно увеличивается число способов и средств, с помощью которых люди общаются, предают данные, осуществляют голосовую и видео трансляции, обеспечивают связь в чрезвычайных ситуациях и т.д., поэтому легко настраиваемые радиосистемы, требующие минимум затрат средств и ресурсов стали быстро развивающимся бизнесом. Программно-определяемые радиосистемы (software defined radio или SDR) позволяют создать передовое коммуникационное оборудование эффективное по цене, питанию, с широкими возможностями настройки.

К SDR принято относить радиосистемы, в которой некоторые или все функции физического уровня реализуются программными средствами и могут быть программно изменены. Программно-определяемые радиосистемы получаются эффективнее и дешевле. Такие устройства могут иметь несколько режимов работы в различных диапазонах частот и большой набор дополнительных функций за счет обновляемости программного обеспечения. SDR объединяют аппаратные и программные технологии, где все или некоторые из работающих функций настраиваются (изменяются) по средствам программного обеспечения.

Такие устройства обычно могут содержать программируемые логические интегральные схемы (FPGA), цифровые сигнальные процессоры (DSP), процессоры общего применения (GPP), программируемые системы на кристалле (SoC). Использование этих технологий позволяет изменять и расширять функциональные возможности радиосистем без аппаратного вмешательства в схему.

Для производителей радиооборудования и системных интеграторов за счет многократного использования программного обеспечения в различных радио устройствах значительно снижаются затраты на разработку. Удаленное перепрограммирование SDR устройств позволяет исправлять ошибки, которые могут возникать после запуска радиосистемы в эксплуатацию, что сокращает время и финансовые затраты связанные с техническим обслуживанием и эксплуатацией приборов.

Для поставщиков радио услуг SDR технология открывает новые функции и возможности, которые будут добавляться к существующей инфраструктуре, не требуют больших финансовых вложений и позволяют провайдерам радио-услуг модернизировать свои сети. Используя радиосистемы на различных территориях, SDR позволяет удаленно их настраивать и модернизировать, что существенно снижает логистические и эксплуатационный расходы. За счет удаленной загрузки программного обеспечения может быть увеличена производительность системы. Модернизации может внести новые функции, тем самым увеличить доход.

Для конечного пользователя технология SDR позволит снизить цену на радиоустройства и доступ к беспроводным средствам коммуникации.

Технология SDR является ключевой в предлагаемом последующем развитии радиооборудования: адаптивное радио, когнитивное «умное радио» и интеллектуальное радио. Одна из основных задач программно-конфигурируемого радио как раз и заключается в обеспечении предельной гибкости изменения параметров оборудования с целью обеспечить максимальную совместимость радиостанций различных стандартов вне зависимости от метода модуляции рабочего диапазона частот, метода доступа к каналам и т.п. при сохранении всех функциональных возможностей сети связи.

Иванов В.Г., Корякин Д.Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ В СИСТЕМАХ УПРАВЛЕНИЯ СЕТЯМИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящее время наблюдается тенденция к постоянному усложнению системы связи, увеличению количества объектов связи, применению все более технически сложных средств с целью улучшения в первую очередь количественных, а также качественных характеристик и показателей системы связи. Условием эффективного функционирования данной системы является осуществление постоянного и эффективного управления связью на основе данных, поступающих от элементов системы связи, и, таким образом, достижением согласованности всех управляемых элементов. Одним из важнейших элементов системы связи является система управления связью, которая представляет собой совокупность функционально и организационно связанных между собой органов, пунктов управления связью и технической основой системы управлению связью.

Различают следующие виды управления связью: организационное, оперативно-техническое и технологическое. Технологическое управление представляет собой третий уровень управления на котором осуществляется изменение маршрутизации, коммутация каналов, соединение абонентов, изменение режимов работы средств связи, контроль их состояния и диагностика. При этом, на фоне внедрения новых инфотелекоммуникационных технологий снижается время, необходимое для реконфигурации системы, повышается обоснованность принимаемых решений. Возникает противоречие, которое заключается в необходимости создания и внедрения единой, унифицированной системы контроля, мониторинга и управления, функционирующей в рамках системы управления связью, которую невозможно реализовать в условиях использования широкой номенклатуры разнотипного оборудования и технологий передачи данных. Таким образом, формируется задача создания системы мониторинга и управления, которая позволит осуществлять контроль, сбор и анализ данных, а также дистанционное изменение состояния элементов и узлов сети с целью обеспечения требуемых задач. Объектом контроля при этом могут быть различные сети связи, тракты и каналы, абонентское оборудование.

Перспективным видится создание или адаптация под требования, предъявляемые к системе связи ВС РФ, системы управления связью, функционирующей на едином стеке протоколов, обеспечивающем унификацию по отношению к агентам сети и позволяющем легко масштабировать и реконфигурировать систему в короткие сроки.

В общем виде, система мониторинга и управления состоит из следующих основных подсистем: подсистема сбора данных, подсистема хранения данных, подсистема анализа данных, подсистема оповещения и информирования, подсистема вывода и подсистема коррекции. При этом элементы подсистемы сбора данных выступают в качестве измерительных устройств, а элементы подсистемы коррекции – в качестве управляющих. Необходимость унификации используемых протоколов состоит в повышении надежности системы управления связью в целом и повышению уровня автоматизации при построении сети, либо изменению ее элементов. Например, внедрение протоколов SNMP и NetFlow позволит эффективно следить за каждым устройством сети и оперативно отслеживать изменения его состояния, вести учет трафика, строить графики производительности, определять нагрузку, в независимости от типа и назначения контролируемого оборудования, а открытость данных протоколов предопределяет их перспективную адаптируемость к специальному оборудованию связи.

Ильина О.Б., Купчиненко О.П., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Большая трудоёмкость решения задач управления в условиях крайнего дефицита времени, отводимого на планирование операций, резко обостряют глобальную проблему полноты и своевременности обработки информации в автоматизированных системах специального назначения (АС СН). При этом большинство задач управления СН требуют для своего решения информацию о местности, подготовка и обработка которой до сих пор частично выполняется традиционным способом, т.е. вручную.

Автоматизация процессов управления в АССН требует применения геоинформационных технологий (ГИТ) обработки картографических данных, представленных в электронном виде. ГИТ – это информационные технологии обработки географически организованной информации.

Сущность ГИТ проявляется в её способности связывать с картографическими (графическими) объектами некоторую описательную (атрибутивную информацию, в первую очередь, алфавитно-цифровую, и иную графическую, звуковую и видеоинформацию). Как правило, алфавитно-цифровая информация организуется в виде таблиц реляционной базы данных (БД). В простейшем случае

каждому графическому объекту ставится в соответствие строка таблицы – запись в БД. Использование такой связи открывает достаточно богатые функциональные возможности ГИТ. Эти возможности различаются в разных системах; то есть, базовый набор функций, например, возможность ответа на вопросы "что это?": указание объекта на карте и "где это находится?" - выделением на карте объектов, отобранных по некоторому условию в БД. К базовым можно также отнести ответ на вопрос "что рядом?" и его различные модификации.

ГИТ предоставляют должностным лицам органов управления свой "картографический интерфейс" для организации запроса к БД вместе со средствами генерации "графического" отчета. ГИТ добавляет обычным системам управления базами данных (СУБД) совершенно новую функциональность – использование пространственных взаимоотношений между объектами. ГИТ позволяет выполнять над множествами картографических объектов операции, подобные обычным реляционным операциям. Эти операции называются оверлейными.

В настоящее время наблюдается тенденция возрастания роли ГИТ в процессе активизации информационных ресурсов, т.к. огромные массивы картографической информации эффективно переводимы в активную машиночитаемую форму только с помощью ГИТ. Кроме того, в ГИТ цифровая карта местности становится динамическим объектом.

Это обусловлено следующими новыми возможностями ГИТ:

- изменяемостью масштаба;
- преобразованием картографических проекций:
- варьированием объектным составом карты;
- "опросом" через карту в режиме реального времени многочисленных БД, содержащих изменяемую информацию;
- изменением способа отображения объектов (цвет, тип линии и т.п.).

По оценкам специалистов применение ГИТ в автоматизированных системах специального назначения позволит повысить эффективность управления войсками и связью с использованием электронных карт на 40% и более.

Киреев С.Х.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

В условиях информационного противоборства информационно-телекоммуникационные сети военного назначения (ИТКС ВН) подвергаются различным информационным воздействиям (ИВ), которые могут нарушить работу системы. Одним из наиболее важных классов ИВ являются удалённые сетевые атаки. Обнаружение таких атак является одной из приоритетных задач обеспечения информационной безопасности ИТКС ВН.

Традиционные системы обнаружения атак (СОА) основаны на использовании сигнатурных и статистических методов, что является проверенным способом для обнаружения известных видов ИВ, таких как использование известных уязвимостей программного обеспечения (ПО) или используемых протоколов, атаки отказа в обслуживании и др., но, так как количество найденных уязвимостей в протоколах, вредоносного ПО и способов обхода различных средств защиты информации (СЗИ) постоянно увеличивается, этого недостаточно для поддержания желаемого уровня защищённости ИТКС ВН.

Одним из возможных способов повышения эффективности работы СОА является использование методов машинного обучения для обнаружения ИВ, а в частности искусственных нейронных сетей (ИНС). Нейронные сети могут использоваться как основное ядро СОА, а могут применяться в качестве дополнительного модуля, расширяющего функционал СОА, использующей другие методы обнаружения атак.

ИНС, анализируя сетевой трафик в реальном времени, принимает в качестве входных параметров различные поля пакетов TCP/IP и делает выводы о том, является ли состояние (поведение) сети в текущий момент времени нормальным, или же она находится под атакой злоумышленника.

Классическая модель нейронной сети – многослойный персептрон (MLP) – обладает одним существенным недостатком: она не позволяет работать с потоковыми данными, к которым непосредственно относится сетевой трафик. Т. е. такая сеть способна делать выводы только на основе одного набора входных параметров.

Учитывая динамический характер функционирования ИТКС ВН такой подход не приемлем, поэтому в качестве решения данной проблемы предлагается использовать более сложный класс нейронных сетей – рекуррентные нейронные сети (РНС). Отличие данного класса ИНС состоит в том, что в них имеется обратная связь: выходы нейронов скрытого слоя сети соединяются с входами сети,

т. е. при обработке нового набора входных параметров учитывается контекст, возникший в процессе обработки предыдущих наборов.

Главными преимуществами использования ИНС в СОА являются:

– Адаптивность системы, позволяющая обнаруживать не только известные виды ИВ, но и ИВ, отличающиеся от нормального поведения по каким-либо косвенным признакам. Таким образом, система сможет обнаруживать не только известные ей атаки, а все атаки, характеризующиеся тем или иным отклонением в поведении сети от нормального.

– Скорость работы системы, обеспечивающаяся тем, что нейронная сеть не осуществляет глубокого анализа проходящих через неё данных. Её основной задачей является анализ различных взаимосвязей и закономерностей данных без учёта их семантики.

Таким образом, можно сделать вывод о том, что использование ИНС является перспективным направлением развития СОА, позволяющим значительно повысить их эффективность и расширить их функционал.

Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Санкт-Петербургский государственный экономический университет,
Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМ СОХРАНЕНИЯ ДАННЫХ

Практически во всех сферах жизни, начиная со сложнейших исследований в различных областях науки и заканчивая оплатой коммунальных платежей, используются информационные системы, работающие с различными типами специализированных и пользовательских данных. Сохранение таких данных является важнейшей задачей, решение которой обеспечивает надежную работу информационных систем и, как следствие, удовлетворение информационных потребностей пользователей.

Для сохранения огромного количества информации на длительное время требуются огромные затраты ресурсов, в первую очередь – физических. Задача системы сохранения данных состоит в минимизации затрат этих ресурсов при сохранении качества предоставления информационных услуг. Для решения таких задач необходимо предусмотреть соответствующие модели управления ресурсами систем сохранения данных.

В докладе рассматривается:

– место процессов сохранения данных в общей структуре ИТ, базовые информационные процессы,подробно рассматривается процесс сохранения.

– законодательство Российской Федерации в отношении хранения информации, в том числе последствия принятия Федерального закона №374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

– технологии больших данных BIG DATA и DATA MINING, также технологии DAS, NAS, SAN и, на физическом уровне RAID.

Предлагается разделить сохраняемые данные, в зависимости от назначения на следующие категории:

1)данные, изначально сохраняемые для передачи будущим поколениям («резервный архив»);

2)корпоративные данные;

3) личные данные.

Остальные характеристики данных рассматриваются во взаимосвязи с назначением.

Предлагается общая структура системы сохранения данных. В связи с различным назначением данных система длительного сохранения должна быть многоуровневой. Каждый уровень предполагает свои технологии хранения.

Распределение информации по уровням должно происходить в зависимости от времени хранения данных, их формата и частоте обращения к ним. Уровень системы, на котором будут храниться данные, определяется характеристиками данных.

Кораблин В.О., Логинов А.А., Мач Д.П., Таран В.В., Труфанов С.К., Шерстюк М.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

ОПЕРАТИВНЫЙ КОНТРОЛЬ И РЕТРОСПЕКТИВНЫЙ АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОТЕЛЕКОММУНИКАЦИЙ

Очевидно, что для полноты оценки защищенности системы недостаточно рассматривать текущее состояние каждого технического или программного средства по отдельности. Полнота и объективность оценки может быть достигнута только при одновременной обработке интегрированных

сведений от множества гетерогенных источников с последующим ретроспективным анализом консолидированных данных.

Реализация такой оценки предполагает наличие системы управления событиями информационной безопасности (ИБ), включающей: средства сбора данных (ССД), технологическую (ТПС) и аналитическую подсистемы (АПС).

Средства сбора данных обеспечивают взаимодействие с гетерогенным, потенциально динамическим множеством источников данных и выполняют сбор событий мониторинга безопасности от этих источников, в качестве которых могут выступать программные и технические ресурсы инфотелекоммуникационной сети.

Технологическая подситсема обеспечивает управление средствами сбора данных, первичную обработку, категоризацию, приоритезацию событий мониторинга безопасности и периодический опрос средств сбора данных, реализуя таким образом оперативный мониторинг событий безопасности инфотелекоммуникаций.

Аналитическая подсистема позволяет на основе данных мониторинга событий безопасности проводить ретроспективный анализ защищенности инфотелекоммуникационной сети, выявлять инциденты ИБ, уязвимости, а также представлять результаты событийного мониторинга ИБ в наглядной для должностных лиц (ДЛ) форме (в виде графиков, таблиц, диаграмм).

Такое построение системы управления событиями ИБ обеспечит как оперативную оценку защищенности – оценку, приближенную к реальному времени за счет функционирования средств сбора данных и ТПС, так и проведение ретроспективного углубленного анализа защищенности системы – за счет АПС.

Использование подобной системы управления позволит повысить общую защищенность инфотелекоммуникационной сети, через полноту и всесторонность анализа получаемых событий, так и упростит процесс выработки решений по реагированию на угрозы ИБ, через представления результатов анализа ДЛ в удобной для них форме.

Кораблин В. О.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

СПОСОБЫ КОНТРОЛЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ ИНФОТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Современные инфотелекоммуникационные сети (ИТКС) относятся к классу сложных организационно-технических систем, и характеризуются иерархичностью, территориальной распределенностью и гетерогенностью.

Также, такие системы обладают повышенными требованиями к информационной безопасности (ИБ), что обусловливается уязвимостью подобных систем в силу разнородного и потенциально неопределенного парка телекоммуникационных средств (ТКС) и программного обеспечения (ПО).

Тогда можно утверждать о необходимости построения собственной подсистемы защиты информации (ЗИ). Также в рассматриваемых ТКС могут функционировать различные системы управления (СУ), образующих подсистему управления данными, и обеспечивающие контроль и восстановление работоспособности элементов системы.

Данные СУ являются источником данных для подсистем ЗИ и предоставляют сведения о функционировании и инцидентах ИБ закрепленных за ними элементов ИТКС.

Однако СУ нацелены, в первую очередь, на поддержание ИТКС в работоспособном состоянии (то есть обеспечение функционирования) и оперируют только теми данными, которые необходимы для обеспечения функций контроля и управления.

Следовательно, получаемых от СУ сведений может быть недостаточно для оценки и контроля защищенности ИТКС и необходимо получение дополнительных сведений. К таким сведениям могут относиться:

1) Журнал событий операционной системы;

2) Внутренний журнал событий ТКС;

3) Значение контрольной суммы конфигурации внутреннего ПО ТКС.

Следовательно, для контроля параметров ИБ элементов ИТКС целесообразно исследовать следующие способы получения указанных параметров:

1) Событийный и параметрический мониторинг на основе данных, получаемых от СУ;

2) событийный и параметрический мониторинг на основе данных, получаемых от ТКС и их внутреннего ПО;

3) Событийный мониторинг журналов событий;

4) Комбинируемый, на основе всех вышеприведенных.

Перечисленные способы контроля позволяют получить целостную и непротиворечивую картину для ИТКС и образующих ее элементов с позиции контроля безопасности информации.

Корень М.Ю., Паршин С.И., Захаров Р.В., Гайнуллин Р.Р.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МОДЕЛИ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

В современных условиях применения высокотехнологичных средств вооруженной борьбы, в качестве особой, новой угрозы на первый план выступает угроза информационной безопасности государства. Ряд ведущих стран мира ведут интенсивную подготовку к информационным войнам. Уже сейчас элементы этих войн становятся обязательными факторами, предшествующими и сопровождающими силовые формы вооруженной борьбы.

Несмотря на то, что в указанных условиях создаются и целенаправленно развиваются отечественные защищенные программные и программно-технические комплексы и средства, являющиеся основой для построения защищенных автоматизированных систем, существует потенциальная возможность несанкционированного воздействия на них деструктивных программных воздействий (ДПВ).

С помощью ДПВ вероятный противник может реализовать опосредованный несанкционированный доступ (НСД), то есть НСД, реализуемый не напрямую, а путем запуска в автоматизированную систему постороннего программного обеспечения – программных закладок, либо внедрения его на этапе проектирования автоматизированной системы.

Результатом воздействия программных закладок являются частичное (полное) блокирование работы системы, генерирование деструктивных команд операционной системе, изменение алгоритмов функционирования прикладных программ, считывание паролей и несанкционированный доступ к закрытой информации, обход программно-аппаратных средств криптографического преобразования информации и другие.

Воздействия программных закладок обладают вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень их опасности, выбрать и реализовать меры защиты. Для исследования и определения ВВХ программных закладок необходима разработка их моделей воздействия.

С этой целью предлагается использовать профильные модели воздействий и метод топологического преобразования стохастических сетей (ТПСС) [1].

Профильная модель – условное представление (последовательность действий или алгоритм) реального объекта, системы или процесса (компьютерных атак) в форме, которая создается для более глубокого изучения их функционирования.

Стохастическая сеть – совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы.

В методе ТПСС исследуется не система, а целевой процесс, который она реализует. Этот сложный процесс декомпозируется на элементарные, каждый из которых может характеризоваться функцией распределения времени его выполнения, плотностью вероятности, вероятностью или средним и дисперсией времени выполнения.

Сущность метода ТПСС состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации, т.е. реализации анализируемого процесса.

Анализ вероятностно-временных характеристик воздействия программных закладок позволит обосновать направления разработки системы защиты ИТКС, целью которой является предотвращение (затруднение) реализации деструктивных программных воздействий.

Коряковцев А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

КРАТКИЙ АНАЛИЗ ОШИБОК СЛЕДЯЩИХ ИЗМЕРЕНИЙ РАЗВЕДЫВАТЕЛЬНЫХ КОМПЛЕКСОВ

Сложность создания многоцелевых радиолокационных комплексов разведки и контроля стрельбы (РКР), удовлетворяющих требованиям современных боевых действий, обусловлена, во-первых, тем, что эти комплексы должны обнаруживать, распознавать и определять с высокой точностью координаты множества малоразмерных целей в сложной обстановке (при наличии радиоэлектронного и огневого противодействия, многолучевого распространения радиоволн, значительной тропосферной рефракции, мощных пассивных помех и пр.). Во-вторых, многоцелевой радиолокационный комплекс разведки и контроля стрельбы должен при минимуме затрат времени автоматически определять координаты огневых позиций противника с учётом данных о рельефе местности и передавать эти данные в систему управления огнём. В-третьих, комплекс для разведки позиций огневых средств противника должен обладать высокой боеготовностью, мобильностью, малым весом и габаритами.

Основным показателем качества радиолокационных комплексов разведки и контроля стрельбы является точность. Точность РКР определяется, в основном, следящим измерителем направления (СИН) и дальности (СИД). У современных РКР она достигает нескольких десятков метров на дальностях до 30 км.

Ограниченный порядок астатизма следящего измерителя приводит к появлению динамической ошибки, которая при известной траектории цели и параметрах следящего измерителя может быть учтена.

Шумы цели также приводят к ошибкам следящего измерителя направления и следящего измерителя дальности. Амплитудный шум цели слабо влияет на работу СИД и моноимпульсных СИН. Но при наличии ошибки запаздывания в следящем измерителе приводит к дополнительной ошибке, величина которой существенно зависит от быстродействия схемы АРУ и составляет единицы процентов от ошибки запаздывания. АШ обычно учитывают на больших и средних дальностях. Шум дальности, доплеровский шум и поляризационный шум цели при оценке точности РКР могут не учитываться.

Канал передачи для РКР, работающих в нижнем слое тропосферы, является источником значительных ошибок. Наибольшее влияние при этом оказывает тропосферная рефракция. Для оценки ошибок, обусловленных рефракцией, необходимо знать значение преломления воздуха n, являющегося функцией географического положения пункта на земной поверхности, погоды, времени года и суток.

Систематические ошибки, обусловленные рефракцией, можно скорректировать путем применения рефракционных профилей, основанных на метеоданных. При этом ошибка по дальности может быть сведена до долей метра, но для этого необходимо знать параметры атмосферы на всех участках траектории цели. В полном объеме эта задача может быть решена лишь в условиях полигона. Частичная компенсация ошибок может быть проведена путем использования метеоданных в месте расположения РКР.

Систематические ошибки, обусловленные несовершенством аппаратуры РКР, могут быть определены методами полунатурного моделирования и натурных испытаний и использованы для коррекции выходных данных РКР.

Купчиненко О.П., Скоропад А.В., Ильина О.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПУТИ РЕШЕНИЯ ПРОБЛЕМНЫХ ВОПРОСОВ ФОРМИРОВАНИЯ, ВЕДЕНИЯ И РАСПРОСТРАНЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЩЕГО ПОЛЬЗОВАНИЯ

Отсутствие совместимости большинства автоматизированных систем, особенно на информационном уровне, приводит к возникновению таких проблем, как различная степень актуальности одних и тех же данных в разных системах, снижение достоверности данных, недостаточная полнота информации, несопоставимость данных и других. Эта проблема усугубляется резким увеличением объема и разнородности информации, содержащейся в автоматизированных системах и необходимой для решения задач управления.

Одним из путей решения данной проблемы является создание единой информационной основы автоматизированных систем. В качестве ее системообразующих элементов предлагается использовать совокупность информационных ресурсов общего пользования, таких как классификаторы различных категорий, нормативно-справочная информация и различные словари. Эти информационные ресурсы являются ключевыми для обеспечения информационного взаимодействия как органов управления, так и автоматизированных систем.

Однако, состояние дел по вопросам формирования, ведения и распространения информационных ресурсов общего пользования в настоящее время нельзя признать удовлетворительным. В частности, отсутствует единая система классификации и кодирования информации, пронизывающая всю структуру системы управления. Большинство пользователей (органов управления и организаций) не могут получить необходимые им для работы классификаторы официальным путем. В результате отсутствует одномоментная идентичность одинаковых классификаторов в различных автоматизированных системах.

Для упорядочения формирования, ведения и распространения информационных ресурсов общего пользования возможно использование организационных и технических подходов.

В рамках организационного направления необходимо создать специализированную службу, предназначенную для организации и осуществления централизованного предоставления пользователям информационных ресурсов общего пользования. Основными функциями службы должны стать:

- получение актуальных версий информационных ресурсов общего пользования из организаций, ответственных за их формирование и ведение;
- ведение фонда информационных ресурсов общего пользования;

– предоставление информационных ресурсов из фонда органам управления и организациям в соответствии с их информационными потребностями и правами доступа.

Техническое направление связано с разработкой специализированных программно-технических средств, обеспечивающих решение стоящих перед службой задач, а также установление единого формата обмена информационными ресурсами общего пользования.

Рациональное сочетание организационных и технических подходов к формированию, ведению и распространению информационных ресурсов общего пользования позволит обеспечить их одномоментную идентичность в различных автоматизированных системах, что создаст условия для обеспечения их информационной совместимости. Все это в конечном итоге позволит повысить качество информационной поддержки процессов управления.

Купчиненко О.П., Скоропад А.В., Ильина О.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ АЛГОРИТМОВ ОЦЕНКИ КАЧЕСТВА ОБСЛУЖИВАНИЯ В СЕТЯХ БЕСПРОВОДНОГО ДОСТУПА

Развитие новых сетевых технологий привело к повсеместному распространению сетей с коммутацией пакетов. Потоковые задачи при проектировании этих сетей решаются, как правило, на основе классической теории телетрафика, в которой наиболее распространенной моделью является простейший или пуассоновский поток, достаточно адекватно описывающий системы распределения информации применительно к речевому трафику в сетях с коммутацией каналов. Однако, для сетей с коммутацией пакетов подобная аппроксимация приводит к излишне оптимистичному прогнозу.

Выявлено, что потоки в сетях с коммутацией пакетов имеют иную структуру. Установлено, что трафик в таких сетях является «самоподобным», то есть выглядит почти одинаково на временной оси, имеет последействие (память) и характеризуется высокой «пачечностью». Привычные алгоритмы обработки трафика, созданные для работы с простейшими потоками, оказываются недостаточно эффективными для потоков с самоподобием. Таким образом проблема самоподобия телетрафика до сих пор не утратила своей актуальности.

В настоящее время широкое распространение получило семейство протоколов IEEE 802.11, реализующих в сетях беспроводного доступа с коммутацией пакетов метод CSMA/CA (множественный доступ с прослушиванием несущей и избежанием коллизий). В связи с тем, что такие сети предоставляют услуги по передаче данных, пакетной телефонии, потокового видео, служебной информации, а также основываясь на результатах экспериментальных исследований, можно говорить о проявлении у трафика этих сетей свойства самоподобия, при котором коэффициент использования канала, описываемый параметром H, превышает 0,5.

Параметр H, называемый параметром Херста или параметром самоподобия, представляет собой ключевую меру самоподобия, или точнее меру длительности долгосрочной зависимости стохастического процесса. Значение $H \leq 0,5$ указывает на отсутствие долгосрочной зависимости. Чем ближе значение H к 1, тем выше степень устойчивости долгосрочной зависимости. Таким образом, при моделировании источника абонентской нагрузки необходимо учитывать долгосрочную зависимость характеристик потока данных сетей беспроводного доступа.

В связи с тем, что этот подход не получил широкого освещения в работах по теории телетрафика, для расчета предполагаемой нагрузки в сетях беспроводного доступа в настоящее время пользуются распространенной формулой Эрланга для систем с отказами, позволяющей определить вероятность поступления заявки в момент, когда все каналы заняты. Данная формула Эрланга является табулированной и связывает вероятность отказа p со значениями нагрузки A и числом каналов n.

Очевидная сложность процедуры определения нагрузки в случае самоподобного трафика непосредственно при помощи этой формулы не позволяет рекомендовать ее для инженерного расчета и в целом для оценки качества обслуживания в беспроводных сетях.

Проведенный выше анализ алгоритмов оценки качества обслуживания в беспроводных сетях вызывает необходимость разработки более адекватных, подходов к оцениванию качества обслуживания применительно к существующим технологиям беспроводного доступа.

Курашев З.В., Горячая А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МЕТОДИКА ОПТИМИЗАЦИИ СЕТЕВОЙ СТРУКТУРЫВ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Основная цель функционирования системы управления сетью передачи данных (СПД) заключается в обеспечении требуемого состояния СПД при своевременном и обоснованном формировании решений в условиях ограниченности вычислительных и временных ресурсов на

принятие решений, а также высокой динамики изменения состояния СПД и разнородности внешних воздействий.

Большое развитие и возрастающее применение находят в предметных областях сетевые структуры и рост интереса к сетевым моделям в управлении.

Сетевая структура моделируется графом, вершины которого соответствуют узлам, а ребра отображают взаимодействие между узлами. Взаимодействие узлов заключается в передаче сообщения другому и получении ответа от него.

Разработана методика построения многоуровневых моделей сетевых структур, на основе иерархической системы вложенных потоковых моделей. При этом формализация задачи оптимизации сетевой структуры определенного уровня осуществляется на основе решения оптимизационных задач на более низких уровнях иерархии.

В частности, решение задачи оптимизации управления маршрутизацией пакетов обеспечивает формирование корректного показателя эффективности функционирования сети передачи данных на более высоких уровнях функциональной архитектуры. Алгоритмы оптимизации, на основе которых предложена методика построения многоуровневых моделей сетевых структур, обеспечивает выполнение процессов управления установлением связи и динамического управления потоками информации, которые планируется реализовать программно.

Курашев З.В., Горячая А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АЛГОРИТМ ОПТИМИЗАЦИИ СЕТЕВОЙ СТРУКТУРЫ В СИСТЕМЕ ОБМЕНА ДАННЫМИ

Для построения алгоритма оптимизации детализируем соотношения для участвующих в задаче функций распределения вероятностей (ФРВ).

Для объектов сети, выполняющих функции передачи пакетов (каналов передачи данных - КПД) или коммутации (центров коммутации пакетов - ЦКП), определяется алгоритмом работы этих объектов и свойствами информационного потока. Как правило, при решении подобных задач эти распределения полагаются экспоненциальными, а потоки – пуассоновскими, однако, как отмечается в ряде работ, их конкретный вид практически не влияет на свойства распределений $P\{t_{п}(\mu) \le \tau\}$ для маршрутов μ и, более того, – на ФРВ $P\{t_{п} \le \tau\}$ для сети в целом. Это обусловлено тем, что в силу центральной предельной теоремы распределение времени задержки пакетов на маршрутах с числом ретрансляций более 4 приближается к нормальному распределению с суммарными математическим ожиданием и дисперсией. При этом финальное распределение $P\{t_{п} \le \tau\}$ с практически необходимой точностью может быть аппроксимировано нормальным законом даже для сетей сравнительно небольших размерностей. Поэтому в расчетах будем использовать экспоненциальное распределение времени задержки в линиях и узлах сети и нормальное распределение для суммарного времени задержки при прохождении пакетов по маршрутам сети.

Анализ особенностей решаемой задачи показывает, что весьма эффективными для нахождения оптимальной функции распределения потоков S могут быть алгоритмы с последовательной локализацией области поиска, однако при этом значительную сложность представляет определение границ этой области. В связи с этим при вычислениях использовались различные варианты приближения функций, которое, с одной стороны, является достаточно точным в области $S(C)$ и, с другой, – в силу гладкости обеспечивает корректную работу алгоритма вне данной области. Кроме того, в построенном алгоритме в отличие от других алгоритмов переход в новую точку осуществлялся без предварительного вычисления градиента в исходной точке, а оценивался по результатам всех предыдущих вычислений функционала $Q(S|C, \Lambda)$. Это позволило существенно сократить время нахождения ε-оптимальной сетевой структуры за счет исключения сложной процедуры вычисления на каждом шаге приращений величины $Q(S|C, \Lambda)$ за счет приращения потока на каждом маршруте. Так, для сетей с общим числом маршрутов $M = 1000 – 2000$ такая модификация алгоритма последовательной локализации области поиска обеспечила сокращение времени решения задачи в 50 – 100 раз.

Курбатов Е.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ТУРБОКОДИРОВАНИЕ И ВОЗМОЖНОСТЬ ЕГО ПРИМЕНЕНИЯ В СЕТЯХ ВОЕННОЙ СВЯЗИ

В Вооруженных Силах Российской Федерации проводятся масштабные работы по реализации комплекса целевых программ, направленных на качественное переоснащение вооруженных сил в соответствии с требованиями, определяемыми концепциями их развития.

Создание единой инфотелекоммуникационной технологии для всех видов и родов войск ВС РФ позволит уменьшить несогласованности в системе управления и, как следствие, сделать её стабильнее. Разрабатываемая система будет состоять из множества разнородных подсистем

управления. Формирование единого информационно-коммуникационного пространства основывается на комплексном внедрении новейших цифровых технологий.

Встает вопрос о необходимости исследования возможности по доработке новейших и показавших себя с лучшей стороны технологий и соответствия их военным требованиям по помехоустойчивости, электромагнитной совместимости, требований по помехо- и разведзащищенности, по безопасности, управляемости и взаимодействию с унаследованными сетями. Одной из таких является стандарт четвертого поколения мобильной связи - технология LTE-Advanced, которая стандартизирована 3GPP как главное улучшение стандарта Long Term Evolution (LTE). Отличается от LTE большей скоростью передачи данных и возможностью распределенно транслировать один и тот же сигнал сразу по нескольким диапазонам. Также LTE-Advanced поддерживает возможность ретрансляции — выход в сеть одного устройства через другое.

Применяемое в технологии LTE-Advanced помехоустойчивое кодирование представляет собой одну из основополагающих процедур процесса подготовки исходной информации перед передачей данных по телекоммуникационным каналам связи. Применение различных по свойствам и методам формирования корректирующих кодов позволяет обеспечить структурированную защиту исходной информации за счет автоматизации процессов выделения и исправления некорректных (ошибочных) кодовых последовательностей. Это позволяет минимизировать деструктивное воздействие среды распространения сигнала и удовлетворить заданный уровень достоверности системы обработки и передачи информации.

Последние спецификации LTE-Advanced предполагают основным способом помехоустойчивого кодирования, используемых при формировании сигналов, турбокодирование.

Среди всех практически используемых современных методов коррекции ошибок турбокоды наиболее близко подходят к границе Шеннона, теоретическому пределу максимальной пропускной способности зашумленного канала. Турбокоды позволяют увеличить скорость передачи информации, не требуя увеличения мощности передатчика, или они могут быть использованы для уменьшения требуемой мощности при передаче с заданной скоростью. Важным преимуществом турбо кодов является независимость сложности декодирования от длины информационного блока, что позволяет снизить вероятность ошибки декодирования путём увеличения его длины.

Значения достоверности передачи данных указывают на высокую степень эффективности турбокода для применения его в качестве основного средства исправления битовых ошибок в каналах с высоким уровнем воздействия помех, следовательно, и возможности его применения в сетях военной связи.

Липатников В. А., Яцкин А. Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СПОСОБ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ДИНАМИЧЕСКИХ HONEYPOT-СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ

Традиционные средства защиты информации (СЗИ), такие как антивирусное программное обеспечение (ПО), межсетевые экраны (МЭ) и системы обнаружения вторжений (СОВ), как известно, не гарантируют абсолютной защищённости информационных сетей (ИС). Антивирусное ПО, являясь средством реактивной защиты, реагирует только на известные ей виды воздействий. МЭ и СОВ же не лишены уязвимостей, которые могут быть использованы злоумышленником для проникновения в защищённую ИС. Решением данной проблемы могут послужить: совершенствование процесса управления защитой ИС за счет расширения базы сигнатур антивирусного ПО, использования эвристических и статистических методов обнаружения вторжений и др. Но эти методы так или иначе нацелены на конкретные, известные действия злоумышленника.

Предлагаемый способ повышения защищённости ИС основан добавлением на границу ИС так называемой honeypot-сети или сети-ловушки, представляющей собой выделенный сервер, на котором с помощью специального ПО имитируется работа реальной ИС. Этот сервер изолирован от остальных элементов ИС и весь поток данных, проходящих через этот сервер, регистрируется и анализируется. Использование данного подхода позволяет решить две основные задачи:

- Своевременно обнаружить попытку проникновения злоумышленника в ИС;
- Получить данные, которые в дальнейшем могут быть использованы для повышения оперативности управления защищённостью ИС, а именно: сведения о приоритетных целях злоумышленника; сведения о квалификации злоумышленника; сведения о средствах, используемых нарушителем; информация о методах взлома и уязвимостях используемых СЗИ.
- Среди преимуществ данного подхода можно выделить:
- Возможность своевременно обнаружить попытку несанкционированного доступа (НСД) к ИС без ложных срабатываний;

– Централизованное управление системой позволяет легко менять её структуру, подстраиваясь под изменения реальной ИС, а также производить анализ данных, полученных в результате работы системы;

– Проактивная модель работы системы предполагает защиту не только от известных методов воздействия на ИС;

– Изолированность системы от реальной ИС предполагает возможность компрометации системы-ловушки.

Технология контейнерной виртуализации Linux Containers (LXC) позволяет создавать легковесные и изолированные виртуальные машины, использующие общее ядро хостовой операционной системы (ОС). Использование LXC для создания honeypot-сетей значительно упрощает их разработку: легковесность виртуальных машин позволяет разворачивать сложные сети, состоящие из множества узлов, на слабом оборудовании, а наличие механизмов изоляции виртуальных машин как друг от друга, так и от хостовой машины, освобождает от необходимости реализации собственных.

Использование предложенного способа позволяет не только непосредственно повысить защищённость ИС, но и также получить сведения о целях и средствах злоумышленника, которые могут быть использованы для повышения оперативности управления защищённостью ИС путём настройки используемых и добавления новых СЗИ.

Малышев В.С., Пантюхин О.И., Пащенко В.В., Терехин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Функционирование автоматизированной системы управления специального назначения (АСУ СН) базируется на реализации информационных технологий (ИТ) и процессов (ИП), разнообразие которых требует выделения базовых, позволяющих осуществлять типизацию и унификацию проектных решений.

Базовые ИТ строятся на основе базовых ИП, но кроме этого включают ряд специфических моделей и инструментальных средств. Этот вид технологий ориентирован на решение определенного класса задач и используется в конкретных технологиях в виде отдельной компоненты. Среди них можно выделить технологии: офисные, мультимедиа, геоинформационные, защиты информации, CASE-технологии, телекоммуникационные, искусственного интеллекта и др.

Специфика конкретной предметной области находит отражение в специализированных ИТ, например, организационное управление, управление технологическими процессами, автоматизированное проектирование, обучение и др. Среди них наиболее продвинутыми являются информационные технологии организационного управления (ведомственные, корпоративные информационные технологии).

Определим понятия. Концептуальная модель – это описание СУ СН как сложной системы с заданной точностью. В рамках данной модели отображаются все объекты (сущности), ИП, правила выполнения операций, существующая стратегия развития и критерии оценки эффективности функционирования системы. Форма представления модели и уровень её детализации определяются целями моделирования. Информационная модель – подмножество концептуальной модели, описывающая все существующие информационные потоки в СУ СН, правила обработки и алгоритмы маршрутизации всех элементов информационного пространства. Информационная технология – совокупность методов и приёмов получения, обработки, представления информации, направленных на изменение её состояния, свойств, формы, содержания и осуществляемых в интересах пользователей органов управления СУ СН. Можно выделить три уровня рассмотрения ИТ: теоретический, исследовательский, прикладной. Кроме того, необходимо принимать во внимание выполняемые в СУ функции управления: планирование (текущее, среднесрочное, долгосрочное), учёт, контроль, оперативное управление.

Средства реализации ИТ в АСУ можно разделить на методические, информационные, математические, алгоритмические, технические и программные. Можно сказать, что конкретная ИТ определяется в результате компиляции и синтеза базовых технологических операций, «ведомственных технологий» и средств реализации.

Базовый ИП основан на использовании стандартных моделей и инструментальных средств и может быть использован в качестве составной части информационной технологии. В состав базовых ИП входят операции (этапы): извлечение (сбор, ввод) информации; транспортирование информации; обработка информации; хранение информации; представление (вывод, выдача) и использование информации.

Таким образом, моделирование информационных процессов необходимо рассматривать на нескольких уровнях: концептуальном, информационном и технологическом при реализации в конкретных условиях на определенных технических и программных средствах.

Манаськин А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОНТОЛОГИЧЕСКИЙ ПОДХОД К СОЗДАНИЮ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Обоснованность принимаемых решений и степень их реализации в значительной степени зависят от объема знаний, которыми располагают специалисты, и эффективности используемых средств сбора, обработки и доступа к информации.

Особую роль в этом играют информационные системы, реализующие методы и технологии искусственного интеллекта - интеллектуальные системы. Отличительной особенностью интеллектуальных систем является их способность обрабатывать знания - накапливать, получать новые знания, извлекать знания, осуществлять поиск знаний.

Необходимым элементом системы поддержки принятия решений является база знаний. База знаний обеспечивает хранение знаний и доступ к ним в процессе функционирования интеллектуальной системы.

Эффективность функционирования системы поддержки принятия решений (СППР) во многом зависит от полноты, непротиворечивости знаний и свойств модели представления знаний в базе знаний.

В области систем искусственного интеллекта вопросам создания баз знаний всегда придавалось важное значение, однако интенсивное практическое формирование баз знаний началось с развитием онтологии. Важную роль в этом сыграли возможности онтологии интегрировать различные виды знаний и определения (в том числе на предметном языке пользователей), а также создание целого спектра алгоритмических и программных средств построения онтологий и работы с ними.

Наиболее перспективным к использованию в СППР остаются онтологии, основанные на методологии концепт-карт, что обусловлено возможностями аппарата CMAP - структурой построения онтологии, включающей онтологию верхнего уровня, предметной области и прикладные онтологии. Онтологии верхнего уровня описывают основные правила построения, функционирования предметной области, а прикладные онтологии реализуются для выполнения частных (специальных) задач.

Для использования в СППР знаний, представленных в виде онтологий предметных областей, последние формализуются посредством семантического анализатора и в понятном для машины виде поступают в базу знаний. В качестве источника знаний могут использоваться хранилища информации по данной предметной области, информационные каталоги, базы данных, в которых сосредоточена различная информация, а также различная отчетная информация, поступающая от взаимодействующих информационных систем.

Эффективность функционирования интеллектуальной СППР оценивают эксперты на основе анализа принятых решений. Результаты работы интеллектуальной СППР носят более многосторонний характер по сравнению с традиционной информационной системой и позволяют помимо прямых ответов на запросы получать скрытые (неявные) знания.

Таким образом, применение онтологического подхода к обработке, систематизации и накоплению знаний является наиболее перспективным направлением создания и дальнейшего развития интеллектуальных СППР.

Марченко А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ НЕЙРО-НЕЧЕТКИХ СИСТЕМ С ТОЧКИ ЗРЕНИЯ ИХ ПРИМЕНЕНИЯ ДЛЯ УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

В настоящее время искусственные нейросетевые системы это одно из перспективных направлений в области разработки искусственного интеллекта. Особую интерес нейронные сети (далее НС) получили из-за способности обнаруживать неявные закономерности в различных процессах при отсутствии необходимости в понимании этих закономерностей, а также из-за способности к запоминанию представленных образов.

Включение концепции нечеткой логики в НС дает возможность в этой системе иметь дело с человекоподобным процессом рассуждений, закладывать в информационное поле НС априорный опыт экспертов, использовать нечеткое представление информации. На данный момент объединение возможностей нейронных сетей и нечеткой логики является наиболее эффективным подходом к

организации систем интеллектуального анализа различного рода данных. Одним из ключевых назначений нейро-нечётких сетей является извлечение знаний. Они предназначены для реализации нечётких правил на базе нейронных сетей.

Нечеткие нейронные сети призваны объединить в себе достоинства нейронных сетей и систем нечеткого вывода. Они позволяют разрабатывать и представлять модели систем в форме правил нечетких продукций, которые обладают наглядностью и простотой содержательной интерпретации, а также, для построения правил нечетких продукций использует методы нейронных сетей, что является менее трудоемким процессом для системных аналитиков.

Применение нейро-нечетких сетей целесообразно при решении задач, которые характеризуются:

- отсутствием алгоритмов решения задач при наличии достаточно большого числа параметров;
- наличием большого объема входной информации, характеризующей исследуемую проблему;
- зашумленностью, частичной противоречивостью, неполнотой или избыточностью исходных данных.

Перспективным направлением развития региональных телекоммуникационных сетей являются мобильные радиосети (МР), которые могут быть применены в интересах силовых структур и ведомств. Все сообщения, которые передаются в МР, можно разделить на два основных класса. Первый класс – сообщения, которые содержат речь и видеоинформацию и образуют в сети трафик реального времени. Для качественной передачи сообщений первого класса необходимо минимизировать задержку пакетов и ее дисперсию (джиттер), что требует гарантированного выделения соответствующей пропускной способности сети. Второй класс – сообщения которые содержат сигналы управления, текст, изображение, графическая и табличная информация и образуют трафик данных. Что бы обеспечить оперативность доставки сообщений второго класса, необходимо рационально использовать доступную для трафика данных пропускную способность сети.

С этой целью в МР на транспортном уровне требуется осуществлять управление интенсивностью отправки источником информационных сегментов. Идея такого управления заключается в обеспечении соответствия отправки данных узлом-источником и доступной для потока в текущей момент времени пропускной способности сети.

Повысить оперативность доставки данных в региональной телекоммуникационной сети позволяет использование метода нечеткого управления межсегментным интервалом. Существенный недостаток указанного метода заключается в несовершенстве выбора параметров функций принадлежности. Недостаточная точность настройки системы нечеткого управления приводит к появлению неприемлемых ошибок различного вида. Что бы от этого избавиться в МР предлагается осуществлять управление задержкой отправки сегментов на основе применения нейро-нечетких интеллектуальных систем.

Таким образом, использование метода нейро-нечеткого управления интенсивностью отправки данных узлами-источниками в МР позволит уменьшить среднее время передачи сообщений и снижение потерь сегментов при сетевых перегрузках.

Михайличенко Н.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

В современном понимании региональный центр обработки данных (РЦОД) это комплексное организационно-техническое решение, предназначенное для создания высокопроизводительной и отказоустойчивой информационной инфраструктуры. В более узком смысле РЦОД - это помещение, предназначенное для размещения оборудования для обработки и хранения информации. В настоящее время типичный РЦОД состоит из следующих компонентов.

Технический компонент. Он создает условия для эффективной работы центра. Программное обеспечение. Это фактически сервисы инфраструктуры РЦОД и ПО для корректной работы процессов. Организационная среда, которая решает вопросы, связанные с предоставлением IT-услуг.

Процесс создания центра обработки данных включает следующие основные этапы.

Планирование - составление технического задания и выработка плана строительства. Конструирование - согласование всех составляющих РЦОД с целью создания единого комплекса и ввода его в эксплуатацию. Строительство - наиболее тяжелый этап в процессе создания РЦОД. Он сводится к комплектации и поставке необходимого оборудования, монтажу, внедрению основных компонентов, проверке их на функционирование. Эксплуатация - это непосредственное обслуживание комплекса и организация работы подразделений. Модернизация - структурные и технические изменения РЦОД, направленные на улучшение его работы.

По назначению выделяют две группы РЦОД, основные и резервные.

Основной РЦОД включает в себя серверный комплекс, системы хранения данных, резервного копирования, эксплуатации инфраструктуры, информационной безопасности и инженерную инфраструктуру. Все составляющие системы интегрированы между собой и объединены высокопроизводительными каналами.

Резервный РЦОД предназначен для обеспечения непрерывности работы в аварийных и чрезвычайных ситуациях и позволяет осуществлять деятельность, если это невозможно в основном РЦОД. Резервный РЦОД может не являться точной копией основного, но должен дублировать все его основные функции, в отсутствии которых деятельность невозможна.

По типу построения различают стационарные и мобильные РЦОД. Стационарный РЦОД представляет собой здание или его часть с размещённым внутри комплексом информационной, телекоммуникационной и инженерной инфраструктурой. Основной функцией РЦОД является размещение оборудования, необходимого для хранения и обработки информации. Также в центре обработки данных размещаются вспомогательные средства, обеспечивающие его работу. Мобильный РЦОД - это комплекс блок контейнеров смонтированных на базе автомобильной техники размещённых внутри аппаратных комплексов информационной, телекоммуникационной и инженерной инфраструктуры, с возможностью подключения к каналам связи и предназначенный для хранения и обработки информации. МРЦОД выполняется в виде, приспособленном для транспортировки автомобильным, железнодорожным, морским, авиатранспортом и имеющем в своем составе автономный отказоустойчивый комплекс систем инженерного обеспечения. В этом случае можно относительно легко нарастить или сократить ресурсы. Что не возможно в стационарном ЦОД. Блок контейнеры, составляющие мобильные РЦОД связаны электросиловыми цепями, линиями мониторинга, видеонаблюдения, пожарной сигнализации и контроля доступа.

Концепция мобильного РЦОД выработана на двух основополагающих моментах:

Во-первых, на основе анализа современных тенденций развития информационных технологий. Исходя из этого, учтена потребность в разработке таких решений, которые позволяют оперативно (мобильно) разворачивать относительно небольшие по масштабу комплексы информационной, телекоммуникационной и обеспечивающей инфраструктуры. Акцентировано внимание на комплексах, разработка которых, с одной стороны, в стационарном (полномасштабном) исполнении является избыточной, а с другой - требует строительной перепланировки и решения проблем инженерного обеспечения.

Во-вторых, на основе обобщения опыта сотрудничестве с организациями телекоммуникационной отрасли. При этом в компоновке оборудования, технических решениях и конструкции образца мобильного РЦОД учитывается практика проектирования, изготовления, ввода в эксплуатацию и последующего сервисного обслуживания поставляемого энергетического оборудования.

Где бы ни размещалась организация, всегда можно организовать там мобильный центр. Необходимость развертывания оборудования в максимально сжатые сроки или создание новых стоек на короткое время на базе существующих основных и резервных мощностей и компонентов инженерной инфраструктуры при отсутствии помещений либо при несоответствии имеющихся помещений требованиям, предъявляемым к РЦОД.. Среди факторов увеличения мобильных РЦОД можно назвать увеличение количества информации, важность непрерывной работы аппаратуры и оборудования. Таким образом, мобильные РЦОД стали крайне востребованы в полевых условиях.

Михеев А.А., Нешин И.Д., Опарин А.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРОЕКТИРОВАНИЕ УНИВЕРСАЛЬНОГО ФОРМИРОВАТЕЛЯ ДЛЯ ПЕРСПЕКТИВНЫХ СИСТЕМ СВЯЗИ С КОСМИЧЕСКИМИ АППАРАТАМИ

Освоение космического пространства для человечества всегда оставалось важным вопросом. Оно является очень трудным и наукоёмким процессом, требующим колоссальных экономических и трудовых ресурсов и представляет интерес не только для мирных целей, но в равной степени и для военного использования. Такими возможностями вывода спутников на орбиту или отправкой космических аппаратов в космос обладает небольшой ряд стран.

Как мирное, так и военное использование космического пространства, и освоение его посредством космических аппаратов позволяет организовать связь в районах со слабо развитыми или не развитыми вовсе наземными системами связи, а также организовать совместную работу с глобальными системами позиционирования (GPS, ГЛОНАСС), что положительно повлияет на управление и улучшит автоматизацию в Вооруженных Силах Российской Федерации.

В связи с тем, что отправка оборудования в космическое пространство имеет высокие технические требования и экономические затраты, появляется потребность в создании универсальных и эффективных систем связи с космическими аппаратами, которые способны

существенно удешевить стоимость аппаратуры и повысить технические характеристики системы, а также позволит работать аппаратуре как в мирном, так и в военном сегменте.

Необходимо осуществлять качественную передачу данных в наземные центры управления, обеспечивать точное управление космическим аппаратом в космосе, при необходимости проводить диагностику и устранение выявленных неполадок во время полёта, без возврата оборудования на Землю.

Рассмотрен вопрос проектирования универсального формирователя радиосигналов для связи с космическими аппаратами (КА). В результате анализа рекомендаций по организации связи с КА выявлены следующие особенности: необходимость реализации высокого КПД для повышения энергоэффективности бортовых систем, работающих от автономных источников питания; требование сокращения уровня внеполосного излучения для улучшения электромагнитной совместимости в условиях дефицита частотного ресурса; использование спектрально-эффективных радиосигналов (GMSK, FQPSK-KF, T-OQPSK) для оптимизации использования частотного ресурса; необходимость реализации высокой скорости передачи для организации информационного обмена с бортовыми системами КА.

Рассмотрен подход к формированию спектрально-эффективных сигналов на основе введения связи между квадратурным и синфазным каналами формирователя.

Разработана компьютерная модель формирователя, реализующего данный подход. Получены сигналы T-OQPSK, FQPSK-KF, GMSK. Исследованы основные характеристики генерируемых сигналов: пик-фактор, нормированная полоса частот, относительный уровень бокового лепестка спектра. Кроме того, сформированы и проанализированы характеристики глазковых диаграмм (а именно, джиттер и величина относительного раскрытия) этих сигналов.

В ходе проектирования был проведён анализ наиболее часто используемых современных цифровых спектрально-эффективных видов модуляции и выбор наиболее подходящих, для использования в устройстве. При этом учтена специфика применения различных элементарных импульсов, применяемых в современных системах радиосвязи.

В программной форме был смоделирован блок формирования и исследовано поведение сигнала при изменении глубины квадратурных связей, вносящих искусственную межсимвольную интерференцию. Были получены адекватные сигналы при необходимой нормированной частоте.

В рамках эксперимента проведено моделирование разрабатываемого устройства в среде MATLAB. Выполнены исследования эффективности сигналов, получены их временные диаграммы, сигнальные созвездия, спектры плотности мощности, «глазковые» диаграммы. Произведён расчёт полос нормированных частот, относительно длительности символа (1,4 – 2,04), пик-фактора сигналов (1,006 – 1,16), ослабление первого бокового лепестка (28 – 31 дБ), раскрытие «глазковой» диаграммы (0,68 – 1) и полученный нулевой джиттер J (идеальные условия).

Мордовин В.Н., Козевалин А.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРОБЛЕМЫ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Высокие темпы роста объемов электронных документов, создающихся и хранящихся в информационных системах, трудности нахождения, извлечения и предоставления необходимой информации отмечаются как ключевые современные проблемы, присущие отрасли систем электронного документооборота (СЭД) и управления контентом.

Ежегодное удвоение массы мирового электронного содержания обусловлено растущими технологическими возможностями обработки электронного контента, расширением видов (номенклатуры) документов, поступающих в электронные системы хранения, увеличением размеров самих документов. Растет число участников документооборота, работающих с документами и обменивающихся информацией друг с другом в электронном виде. Все более широкие категории людей начинают создавать, публиковать и потреблять документы в электронной среде.

При этом непрерывно возрастают требования к числу и сложности функций и процедур обработки документов, которые информационная система должна брать на себя, способам "обнаружения" электронных документов в корпоративном хранилище, формам предоставления потребителю. Кроме того, множатся внутренние процессы, которые необходимо выполнять информационной системе по обслуживанию данных.

Среди них особое место занимают процессы, связанные с защитой информации. Один из ключевых принципов защиты информации заключается в том, что права доступа к документам должны определяться на уровне документа, а не только баз данных. Списки управления доступом должны быть динамическими и меняться (пересчитываться) — часто многократно, в течение жизненного цикла документа и в связи с изменениями в организационной структуре. Наш многолетний опыт мониторинга крупномасштабных территориально распределенных систем электронного документооборота позволил выделить следующие наблюдения, касающиеся общих

факторов, влияющих на эксплуатационные характеристики систем. Реализация множественных, разнородных, часто взаимно противоречивых требований к СЭД в сочетании с обращением большого количества потребителей с разнообразными запросами к огромным массивам данных и возрастанием внутренней активности информационной системы приводит к экспоненциальному росту нагрузки на систему и соответствующему падению производительности. При определенных соотношениях технических и эксплуатационных характеристик система перестает быть масштабируемой. СЭД достигает порога интенсивности нагрузки, за которым она не может нормально функционировать вне зависимости от предоставляемых ей системных ресурсов. И чем крупнее компания, тем выше вероятность, что этот порог будет рано или поздно достигнут.

В связи с тенденцией массового подключения к СЭД пользователей наблюдается нарастание проблемы удобства работы различных категорий пользователей в системе. Эксплуатационную эффективность СЭД следует оценивать с двух точек зрения:

– с одной стороны, она определяется временем отклика системы на различные действия (запросы) пользователей (быстродействие);

– с другой, — тем, насколько удобно и эффективно пользователь может сформулировать свои запросы к системе, адресовать их и получить адекватный ответ. (в стандарте ISO DIS 9241-11 определяется понятие "ЮЗАБИЛИТИ" как степень, в которой продукт может быть использован определенными пользователями при определенном контексте использования для достижения определенных целей с должной эффективностью, отдачей и удовлетворением.) Однако разные категории участников документооборота по-разному работают с документами. Способы работы пользователей ключевым образом отличаются от подходов, например, менеджеров СЭД. Поэтому и критерии удобства, комфортности, удовлетворенности у разных пользователей разные.

Особенно болезненно проблемы как производительности, так и удовлетворенности пользователей проявляются в условиях территориальной и организационной распределенности.

Мошак Н.Н.
Россия, Санкт-Петербург, ПАО «Интелтех»

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ И ЕЕ ЭЛЕМЕНТОВ

Функциональные модели мультисервисной сети (МСС) связи и ее элементов служат для составления на их базе аналитических моделей соответствующих объектов, учитывающих, на выбранном уровне описания, все необходимые преобразования, которые претерпевает сообщение при прохождении через моделируемую систему.

Основу МСС образует ее инфокоммуникационная транспортная система или ее коммуникационное ядро. Поэтому, при описании процессов, протекающих в МСС на уровне «узел - сеть связи» основное внимание в докладе уделяется составлению функциональных моделей именно этих объектов. При составлении функциональной модели должны учитываться общая «физическая конструкция» моделируемой системы и порядок взаимодействия ее отдельных элементов при прохождении через систему, потоков сообщений различной природы (речь, видео, данные). Степень подробности описания диктуется физическими соображениями и возможностями применения, различных аналитических методов исследования.

Укажем уровни описания и характер решаемых задач, которые необходимо принимать во внимание при построении функциональных моделей сети и ее элементов.

На самом низком уровне, обычно, рассматриваются вопросы моделирования среда распространения сигналов, построение оптимальных методов передачи и приема сигналов в соответствующих средах, выбор формы сигналов, методов регенерации, компенсации искажений, поэлементной синхронизации, изучаются возможности организации приема «в целом» и даются рекомендации по конструкции модемов.

На втором уровне изучаются дискретные каналы (двоичные, m-ичные, кодовые, системные каналы) связи, строятся соответствующие модели дискретных каналов, оцениваются их параметры по реальной статистике, изучаются кодовые методы защиты дискретной информации от ошибок, строятся модели соответствующих систем передачи, рассматриваются и детализируются алгоритмы к каналах и трактах передачи и т.д. На этом уровне (в сочетании с первым уровнем описания) в основном исследуются методы получения максимальной скорости передачи при заданной достоверности. Характеристики каналов передачи информации могут учитываться или при описании входящих потоков информации или вводиться в описание состояния системы при составлении матрицы плотностей перехода.

На третьем уровне рассматриваются вопросы прохождения потоков сообщений через отдельные элементы сети (маршрутизаторы, коммутаторы, концентраторы, абонентские пункты (АП), тракты передачи и т.д.) и всю сеть в целом. Основная задача исследований на этом уровне - это получение вероятностно - временных характеристик МСС и ее элементов (распределение задержек пакетов, эффективная скорость передачи в тракте, вероятность переполнения буферной памяти узлов коммутации, вероятность блокировки, вероятность того, что время задержки пакетов в сети не

превышает заданного значения и т.д.) в процессе ее функционирования. Основной метод исследования - теория массового обслуживания.

На четвертом уровне изучаются общесетевые вопросы, связанные с топологией сети, распределением потоков на сети, управлением сетью и т.д.

Отдельно стоят вопросы организации программного обеспечения узла коммутации, описания его структуры и взаимодействия с его аппаратурным комплексом.

При построении функциональной модели МСС, прежде всего, производят идентификацию моделируемой системы и соответствующей системы массового обслуживания, т. е. выделяют приборы обслуживания, буферные накопители, фиксируют дисциплины занятия обслуживающих приборов, порядок их освобождения, характер управления очередями, формулируют требования к описанию состояния системы и системы приоритетов.

В докладе рассмотрена функциональная модель элемента сети – «узел + исходящие каналы», на базе которой (согласно матрице смежности сети) строится функциональная модель МСС в целом.

Муренин И.Н., Новикова Е.С.
Россия, Санкт-Петербург Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОБНАРУЖЕНИЕ АНОМАЛЬНЫХ СИТУАЦИЙ В СИСТЕМЕ АНАЛИЗА ДАННЫХ

Благодаря широкому распространению мобильных устройств, обладающих возможностью геопозиционирования объектов, растут объемы данных, характеризующих движение объектов во времени и пространстве. Анализ таких данных может быть полезен при решении задач обеспечения безопасности и мониторинга состояния критических инфраструктур. Например, анализ перемещений персонала некоторой организации позволяет оценить соблюдение политик безопасности предприятия, выявить и описать аномальные ситуации, развитие которых может привезти к серьезным последствиям.

Для наглядного представления ключевых особенностей, содержащихся в пространственно-временных данных, существует множество методов визуализации, позволяющих в совокупности с методами интеллектуального анализа данных, продемонстрировать разницу в поведении объектов, построить шаблоны типичного поведения и определить временные интервалы и места, в которых оно сильно отклоняется от нормы. В настоящей работе представляется подход к визуальному анализу траекторий сотрудников компании, отличающийся этапом предварительной обработки исходных данных, позволяющим управлять уровнем детализации данных о перемещениях, задавая различный интервал времени, и фиксировать отклонения объектов с точностью до единицы времени и контролируемой зоны.

Особенностью входных данных является сложность определения расстояния между исследуемыми объектами, поскольку координаты задаются в терминах «этаж-контролируемая зона». Кроме того, логи датчиков близости, фиксирующих перемещения сотрудников, имеют не регулярный характер: временной интервал между значениями может быть равен 50 секундам или 4 часам. Было решено обрабатывать исходные данные таким образом, чтобы для каждого пользователя формировались вектора, отражающие статистику его перемещений по зонам и длительность нахождения в них. Выполнение этих условий обеспечит удобство и наглядность дальнейшей визуализации данных, так как номера зон будут определять структуру анализируемых данных и, соответственно, будет удобно отслеживать изменения посещаемости в любой необходимый интервал времени.

Для обнаружений аномальных ситуаций система анализа данных на первом этапе разбивает объекты на кластеры, используя сформированные ранее вектора, отражающие закономерности в перемещениях сотрудников. В настоящий момент в качестве алгоритмов кластеризации используется алгоритм k-means, который является одним из универсальных методов для работы с временными рядами. Результатом его применения являются кластеры, центроиды которых описываются средними значениями атрибутов принадлежащих ему объектов. Эта особенность полезна при выявлении аномалий в перемещениях среди объектов кластера путем оценки отклонений значений атрибутов отихцентроида. Недостатком алгоритма k-means является необходимость указания числа кластеров вручную, поэтому возникает проблема определения оптимального разбиения. Для решения этой задачи применяется метод, основанный на построении матрицы кластеризации для каждого возможного количества кластеров, вычисления специализированного критерия на каждой итерации и последующей минимизации полученных значений. Качество разбиения на кластеры проверяется с помощью метода иерархической кластеризации с построением дендрограммы, что позволяет выбрать критерий, который лучше всего соответствует структуре анализируемых данных. В дополнение к иерархическим методам кластеризации, применяется методика визуализации перемещений пользователей по контролируемым зонам, основанной на диаграмме Ганта. Для визуализации отклонений используются тепловые карты.

Подходы к визуализации и поиску аномалий тестировались на наборе данных, предоставленном в рамках VASTChallenge 2016. Они описывают перемещения сотрудников организации по зданию в течение двух недель и представляют собой файл, где каждому сотруднику ставятся в соответствие временная отметка и атрибуты зоны, в которой зафиксировано его положение в данный момент времени, всего насчитывается 126 сотрудников.

Неижмак А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ОСНОВНЫХ ХАРАКТЕРИСТИК СИСТЕМ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ В КАНАЛАХ РЕГИОНАЛЬНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ И ПУТИ ИХ СОВЕРШЕНСТВОВАНИЯ

Эффективное использование вычислительной техники в автоматизированных системах управления (АСУ) невозможно без обмена данными между их элементами. Поэтому создание и развитие автоматизированных систем управления привело к появлению и быстрому развитию такого вида электросвязи, как передача данных. Доклад посвящен вопросам повышения эффективности региональных систем обмена данными.

Совокупность комплексов технических средств передачи данных, образующих на основе каналов связи первичной сети определенную структуру, функционирующих по заданным алгоритмам и обеспечивающих обмен данными в АСУ, называют системой передачи данных, или системой обмена данными СОД. В докладе представлено основное назначение и цель функционирования СОД.

Система обмена данными есть совокупность комплексов оконечных средств обмена данными и центров коммутации, соединенных каналами связи, обеспечивающая обмен данными в автоматизированных системах управления при выполнении требований по заданным показателям эффективности.

Проблема повышения достоверности передачи данных обусловлена несоответствием между требованиями, предъявляемыми при передаче данных, сигналов управления, телеграфных и других видов дискретных сообщений, и качеством большинства реальных каналов связи, получаемых при использовании современной каналообразующей аппаратуры.

Решение проблемы повышения достоверности в десятки тысяч раз только путем совершенствования каналообразующей аппаратуры экономически нецелесообразно, а в ряде случаев технически невозможно.

В системах обмена данными повышение достоверности является одной из основных функций каналов передачи данных. Осуществляется оно при обмене пакетами данных между элементами сети передачи данных, а также при обмене сообщениями данных между отправителями и получателями данных.

Огромное значение для развития информатики и телекоммуникаций имеют методы обеспечения достоверного обмена цифровыми данными, среди которых важное место занимают системы повышения достоверности. Системы повышения достоверности информации - это комплекс мероприятий по обнаружению и исправлению ошибок, возникающих при передаче информации по каналам связи в сетях передачи данных. В докладе приведены две группы характеристик систем повышения достоверности, а также принципиальная разница между этими группами.

Для оценки эффективности систем передачи используют вероятностно временные параметры и параметры достоверности системы передачи данных.

Отмечены способы повышения достоверности в однонаправленных системах передачи, а именно:

- помехоустойчивое кодирование;
- многократная передача всего сообщения или его части;
- передача по параллельным каналам связи.

В докладе указано, что перечисленные способы при необходимости могут использоваться комбинированно.

Рассмотрены этапы повышения достоверности в системах передачи данных с обратной связью и отмечена их большая эффективность по сравнению с однонаправленными системами передачи в условиях преднамеренных помех. В зависимости от функций передатчика, приемника и канала обратной связи различают системы с решающей, информационной и комбинированной обратной связью. Дана краткая характеристика каждой из систем.

Приведена классификация систем с решающей обратной связью в зависимости от алгоритма их функционирования. В заключении доклада отмечены результаты сравнительного анализа достоверности передачи систем с ИОС и РОС и приведен предполагаемый вариант ее повышения с минимальным влиянием на скорость передачи данных.

Нешин И.Д., Михеев А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

Информатизация образования – это сложный многоуровневый процесс, который нельзя свести к снабжению школ компьютерами, электронными учебниками и подключению к Интернету. В настоящий период времени необходимо рассматривать и развивать содержательную сторону использования технических средств. Техническое обеспечение, безусловно, является важной, но лишь обеспечивающей основой процесса информатизации.

Внедрение информационных технологий в процесс преподавания всех предметов влечёт за собой необходимость повышения информационной культуры педагога, внедрения новых методов обучения с использованием компьютерных технологий в следующих направлениях: контроль знаний, лабораторный практикум, самообразование (сетевое взаимодействие).

Следует заметить, что любая инновационная деятельность в образовательной сфере должна соответствовать стратегическим целям государства в области образования. Закон Российской Федерации "Об образовании" в качестве основополагающих выдвинул ряд таких целей, среди которых: 1. Формирование системы образования, способной адаптироваться к условиям и нормам жизнедеятельности людей, к новому взаимодействию теории и практики; 2. Внедрение принципов развивающего обучения и методологии деятельностного подхода, превращение образования в среду освоения способов мышления и деятельности.

Основным потенциалом современных компьютеров являются, во-первых, огромные возможности глобальной сети Internet, во-вторых, прикладное программное обеспечение, входящее в пакет Microsoft Office.

Несомненным требованием сегодняшнего дня для всех современных людей является высокая сетевая культура, умение использовать сеть Интернет для поиска, хранения информации, для организации эффективного взаимодействия с другими пользователями сети. Развитие Интернета за последние 2–5 лет в значительной степени осуществляется путем активного внедрения ряда принципов и технологий.

Прикладные программы пакета Microsoft Office позволяют вводить и редактировать любой текст (повышение восприятия и понимание задания учащимися, а также возможность качественно заниматься оформлением творческих работ), создавать и обрабатывать табличные данные (дает большие возможности построения диаграмм и графиков для визуализации и анализа числовой информации), форматировать базы данных, изготавливать буклеты, визитки, приглашения и т.д., создавать и редактировать изображения, создавать и редактировать мультимедийных презентаций.

Таким образом, применение новых информационных технологий на уроках экономики имеет два основных аспекта: компьютер как инструмент изучения экономики и компьютер как средство обучения экономике. Эти аспекты тесно взаимосвязаны в процессе обучения, т.к. любое общение с компьютером предполагает и то и другое.

Нешин И.Д., Опарин А.С., Михеев А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ТЕХНОЛОГИЯ ВИРТУАЛЬНОГО ТУРА КАК ИНСТРУМЕНТ ДЛЯ ОБУЧЕНИЯ

В Военной академии связи был изучен опыт внедрения инновационных технологий в ряде гражданских вузов, промышленности, военных организаций, который позволил внедрить и адаптировать на реальный процесс обучения, технологию, позволяющую интегрировать любые объекты визуализации. Сегодня курсанты работают с текстами, объектами и реальными процессами в единой программной среде.

Отличительными особенностями представленной технологии является:

- высокая визуализация, нелинейность;
- вызов объектов производится мгновенно, путем нажатия на конкретный объект (вызов 3D-ролика);
- в нижней части экрана монитора существует «навигатор», который позволяет быстро найти и вызвать любой из объектов;
- обычно курсанты испытывают наибольшие трудности при изучении данного вопроса;
- при изучении режимов работы станции объектом визуализации является – флэш-схема, которая позволяет изучить процесс формирования сигнала в станции для конкретного режима работы.
- объектом визуализации могут быть сферические 3D панорамы, которые позволяют с высокой степенью детализации изучить и рассмотреть внешний вид станции, размещение и расположение органов управления, рабочего места оператора.

Причем временной ресурс составляет 4 (четыре) учебных занятия, в сравнении с традиционной формой обучения при рассмотрении данных вопросов.

На базе данной технологии в академии операторами научной роты был создана автоматизированная виртуальная система по системам и аппаратным связи, который позволяет ознакомиться с основным оборудованием станций, изучить их работу, а также рассмотреть документацию, инструкции по работе операторов.

Таким образом, технология виртуального тура, на основе которой разрабатывается автоматизированная виртуальная обучающая система, является отличным инструментом для обучения слушателей и курсантов академии. Вместе с тем, поиск технологий и программных продуктов, с последующей адаптацией на реальный учебный процесс достаточно трудоемкий, но имеет свои пути решения. Целью которого станет повышение наглядности представляемого материала и более прочному усвоению обучаемым теоретических основ изучаемой техники и комплексов связи. Посредством игровых методов и технологии виртуального 3D-тура погрузить обучаемого в область предметных знаний. Это позволит преподавателю организовать новые, нетрадиционные виды учебной деятельности, широко использовать методы активного, деятельностного обучения в организации творческой работы слушателей и курсантов.

Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МОДЕЛИ ВИЗУАЛЬНОГО АНАЛИЗА СЕТЕВЫХ ПОТОКОВ КОМПЬЮТЕРНОЙ СЕТИ

В настоящее время методики визуальной аналитики, в которых в равной мере используются достоинства графического представления данных и их автоматизированного анализа, считаются едва ли не единственным способом анализа и исследования данных большого объема. В частности, по мнению Р. Марти, визуализация данных “является единственным подходом, который может быть адаптирован к постоянно меняющемуся ландшафту информационных угроз и вычислительной инфраструктуры”. Это утверждение подтверждается ростом интереса научного сообщества к данной проблеме, проведением ежегодных специализированных международных симпозиумов и/или семинаров в рамках международных конференций, таких как IEEE Conference on Visual Analytics Science and Technology (IEEE VAST); IEEE Symposium on Visualization for Cyber Security (VisSec); Eurovis workshop on Visual Analytics и т.д.

Выделяют семь основных проблем-вызовов, стоящих перед разработчиками моделей визуального анализа: большой объем данных; многообразие источников данных; отсутствие синхронизации между источниками данных; качество данных; формирование ритма сети (формирование паттерна нормального поведения информационной системы); отслеживание угроз и перегрузка информацией. Первые четыре задачи непосредственно связаны с анализируемыми данными, необходимость их предварительной обработкой и синхронизацией во времени. Три других непосредственно связаны с выбором модели визуализации. Причем, модели визуализации должны позволять формировать паттерны, как нормального функционирования сети, так и аномального.

В докладе представлены результаты исследования моделей визуализации, используемых для анализа сетевых потоков компьютерной сети, отражающие, как решаются выше перечисленные задачи. Описаны характерные графические паттерны нормального и аномального поведения информационной системы, зависящие от выбора модели визуализации. Можно выделить два основных подхода к представлению данных о сетевых потоках. В первом случае, исследуется состояние хоста компьютерной сети, и все данные о сетевых потоках оцениваются в рамках одного хоста. В этом случае чаще всего используются пиксель- или глиф-ориентированные представления, поэтому характерные графические паттерны сетевой активности имеют вид множества глифов или цветных точек, форма которого зависит от типа атаки и роли хоста внутри сети. Во втором подходе, акцент делается на представление самих информационных потоков, которые в зависимости от модели представления отображаются в виде линий (графы на параллельных координатах, связные графы) или в виде точек многомерного пространства, в качестве координат которого выступают атрибуты сетевого трафика. Паттерны аномальной сетевой активности имеют вид густо заштрихованных выпуклых многоугольников или скопления точек в виде линий или кривых в многомерном пространстве. В докладе показано, что достаточно простые модели визуализации полезны при выявлении инфраструктурных сетевых атак, таких как DDoS-атаки, сканирование портов и т.д. Однако для анализа сложных многошаговых атак необходимо использовать множество взаимосвязанных моделей визуализации или составные модели графического представления данных, состоящих из нескольких, и позволяющих построить временной профиль компьютерной сети.

В заключении доклада формулируются основные направления будущих исследований, связанных в частности с проработкой вопросов анализа сетевых потоков в облачных вычислительных сетях, интернете вещей (Internet of Things). Следует отметить, что достаточно большая проблема

связана с оценкой эффективности различных моделей визуализации. Результаты, полученные в ходе исследования эффективности на этапе проектирования или уже на этапе оценки прототипа, не позволяют сравнить методики визуального анализа данных между собой, выявить слабые стороны одной модели и сильные стороны другой.

Ноздрачёв Л.И. Бударин Э.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В современном мире, мире инфотелекоммуникацинных технологий, проблемы, связанные с утечкой информации, являются наиболее актуальными. Не зря говорят: «Кто владеет информацией, тот владеет миром».

Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Иными словами, понятие НСД означает состояние незаконного изъятия, уничтожения, изменения и другого вида воздействия на информацию без ведома правообладателя.

В настоящее время обработка конфиденциальной и секретной информации есть неотъемлемая часть каждой успешной организации, в том числе и ВС РФ. Технологии продвинулись до того, что вредоносные закладки могут быть вписаны во flash-память, BIOS и аппаратные средства компьютера. Для того, чтобы кибератака была предотвращена, и нужная информация не смогла бы «утечь», необходимо иметь достаточно надежные и защищенные аппаратные и программные средства. Существует аппаратно-программный модуль доверенной загрузки, предназначенный для защиты автономных и сетевых компьютеров от несанкционированного доступа.

Постоянное совершенствование технологий в области кибератак дает возможность через несовершенство средств доверенной загрузки получить доступ как к компьютеру «жертвы», так и соответственно к данным, составляющих сведения государственной тайны.

Чтобы избежать подобных случаев необходимо как минимум, постоянно искать несовершенства, уязвимости средств - тем самым, идти по пути постфактума, имея в прошлом один или несколько НСД от программ шпионов.

Модуль доверенной загрузки представляет собой комплекс аппаратно-программных средств, устанавливаемый на рабочее место вычислительной системы (персональный компьютер, сервер, ноутбук, специализированный компьютер и др.).

Основная задача модулей доверенной загрузки – создание полноценной доверенной среды на основе анализа состояния и максимальных отказов к системным запросам. Для этого необходимо использовать как расчёты на основе известных статистических моделях оценки надёжности, таких как Миллса, Нельсона, Липова и простой интуитивной модели так и необходимого процесса блокирования новых запросов, тем самым создавая отказ НСД в реальном времени. И здесь нам приходится говорить о ненадёжности программного обеспечения, так как в таком случае в процесс принятия решения о неизвестных действиях все ещё должен участвовать пользователь. Который, в свою очередь, должен как минимум понимать, что происходит с его АРМ.

В простом случае, пользователь является обычным обывателем, не способным оценить угрозу. И поэтому, до появления программ способных самостоятельно принимать решение о вновь выявленных угрозах, программа защиты должна предоставлять пользователю максимальное количество информации об угрозе (её анализа, статистике, возможного направления действий и т.п.) для принятия решения на её уничтожение или использование.

Создание подобного рода программного обеспечения, значительно повысит безопасность систем и косвенно заставит пользователей понимать происходящее.

Овсянников С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПОДХОДЫ К МОДЕЛИРОВАНИЮ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЛАНИРОВАНИИ СЕТИ БЕСПРОВОДНОГО АБОНЕНТСКОГО ДОСТУПА

В настоящее время происходит модернизация систем и сетей связи, связанная с интенсивным развитием компьютерных технологий, цифровой передачи и телекоммуникаций, влияющим на принципы построения и методы планирования сетей беспроводного абонентского доступа (СБАД).

Принципиальным отличием технологий беспроводного от проводного доступа является использование свободного пространства как ненаправленной среды передачи электромагнитных волн. Основными достоинствами беспроводных технологий являются мобильность, оперативность развертывания, слабая зависимость от местоположения, а недостатком - «открытость» к внешним

воздействиям в условиях сложной помеховой обстановки, частично компенсируемой на этапе частотно-территориального планирования.

К основным этапам планирования СБАД относятся: проектирование, оптимизация и поддержка функционирования сети. Важную роль при планировании СБАД играет система поддержки принятия решений (СППР). СППР по планированию СБАД — это система, обладающая средствами ввода, хранения и анализа данных.

Планирование СБАД осуществляется должностными лицами, находящимися на автоматизированных рабочих местах (АРМ), входящих в состав СППР, имеющих кроме технических средств автоматизации, средства программного, информационного и методического обеспечения.

Изменение условий функционирования СБАД способствует воздействие внешних и внутренних дестабилизирующих факторов. Поэтому возникает необходимость динамического управления режимами функционирования СБАД, используя адекватные аналитические модели и алгоритмы вычислений в соответствующих средствах программно-алгоритмической поддержки (СПАП).

Полученные аналитические модели и алгоритмы вычислений отвечают требованиям сложности, точности и скорости, выполнение которых окажет влияние на работу СПАП в СППР при планировании СБАД.

Олимпиев А.А.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

МЕТОДИКА ФОРМИРОВАНИЯ КОМПОНЕНТОВ МЕТАИНФОРМАЦИИ ДЛЯ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ЭЛЕМЕНТА СЕТИ СВЯЗИ С УПРАВЛЯЕМОЙ ТОЧНОСТЬЮ

Компонент метаинформации (КМИ) — совокупность структур данных и алгоритмов их обработки, использующаяся в программных компонентах информационных систем и имеющая конкретное прикладное значение.

Разработка КМИ является достаточно трудоемким творческим процессом, который всегда выполняется с участием эксперта в предметной области, хотя в простейших случаях разработчиком КМИ и экспертом в предметной области может являться одно и то же лицо. КМИ формируется по определенным правилам, которые могут различаться в зависимости от архитектуры и назначения информационной системы, применяемых в ней языков программирования и спецификаций. В то же время совокупность этих правил имеет и общие черты, которые могут быть представлены в виде комплекса методик их формирования, обладающих достаточной степенью общности.

В настоящее время ведутся работы по созданию такого комплекса для АСУ связью. Одной их его составляющих является методика формирования КМИ, предназначенного для автоматической оценки состояния элемента сети в системе оперативно-технического мониторинга.

КМИ, содержащий описание алгоритмов и структур данных, предназначенных для вычисления состояния элемента сети связи, должен включать как минимум следующие составляющие:

- структуру данных «дерево», являющуюся абстракцией иерархии свойств, характерных для класса элементов сети, который используется при моделировании конкретного элемента в информационной системе;
- алгоритмы вычисления значений величин, характеризующих свойства верхних уровней иерархии, по значениям величин, характеризующих свойства нижних уровней иерархии;
- алгоритмы вычисления значений величин, характеризующих простейшие свойства, на которые разлагаются свойства всех верхних уровней иерархии, по данным, полученным в результате мониторинга.

Методика формирования такого КМИ заключается в выполнении последовательности действий, которое приводит к получению всех перечисленных элементов:

- анализ места, роли и назначения элемента сети связи в системе связи;
- анализ данных мониторинга, которые могут быть получены в результате взаимодействия с агентом управления оборудованием (информационной базы управления), либо введены вручную в случае отсутствия агента;
- формирование дерева свойств класса, которому принадлежит элемент сети, и правил вывода свойств нижнего уровня из данных мониторинга;
- задание весовых коэффициентов, характеризующих важность свойств нижнего уровня дерева по отношению к свойствам верхнего уровня, и упорядочивание свойств по убыванию важности;
- выбор для величин, характеризующих свойства, значений по умолчанию, которые будут использоваться при вычислении величин, характеризующих свойства верхнего уровня, в ситуациях, когда свойство нижнего уровня, участвующее в вычислениях, помечено как «не учитывается»;
- формирование алгоритмов вычисления величин, характеризующих свойства нижнего уровня иерархии;
- формирование алгоритмов вычисления величин, характеризующих свойства верхнего уровня иерархии;

– формирование алгоритма вычисления значения точности, с которой производится оценка состояния, по значениям весовых коэффициентов свойств, которые помечены как «учитывается»;
– реализация КМИ с помощью выбранного языка программирования и/или спецификаций;
– формирование документации по применению разработанного КМИ.

Применение КМИ, полученного по описанной методике, позволяет пользователю управлять нагрузкой, создаваемой системой мониторинга на ресурсы сети связи, за счет изменения точности оценки. Пользователь помечает не важные в данный момент свойства элемента сети связи как «не учитываемые», в результате чего система мониторинга прекращает сбор данных, от которых зависят помеченные свойства.

Олимпиев А. А., Шерстюк Ю. М.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

МЕТОДИКА ПОСТРОЕНИЯ И АДАПТАЦИИ СИНТАКСИЧЕСКИ ВАРИАНТНОЙ СИСТЕМЫ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО МОНИТОРИНГА

Система оперативно-технического мониторинга (СОТМ) является составной частью АСУ связью и предназначена для сбора, хранения и обработки данных мониторинга сети связи и предоставления этих данных пользователю для поиска аварийных ситуаций и принятия решений по их устранению. СОТМ строится для повышения качества управления сетями и услугами.

Создание СОТМ как синтаксически вариантной (СВ) информационной системы предполагает применение методологии метауправления функциональностью (МУФ) к ее программному обеспечению.

Суть методологии заключается в применении метода многоаспектного анализа структурных элементов программного обеспечения (структур данных, алгоритмов и связей между ними) с целью отделения управляющих элементов от прикладных с дальнейшим представлением и программной реализацией последних в виде комплекта расширяемых динамически подключаемых библиотек и баз данных с перестраиваемой структурой.

С точки зрения теории управления построение СОТМ является управляющим воздействием на систему связи, выполняемым с целью ее перевода из состояния, в котором СОТМ отсутствует, в состояние, в котором СОТМ имеется и функционирует с заданным качеством. Поскольку СВ СОТМ отличается от традиционной, методика ее построения также специфична, поскольку в ней учтены действия, связанные с метауправлением функциональностью.

Опыт построения СВ СОТМ для различных применений позволил выделить его основные этапы:

– анализ сети связи и ее ожидаемых изменений с целью получения информации о составе узлов и направлений связи и объема телекоммуникационных ресурсов, которые можно зарезервировать под сеть обмена данными СОТМ без ущерба качеству предоставляемых услуг связи;
– анализ сети с целью построения модели предметной области;
– разработка комплекта компонентов метаинформации с описанием начальной структуры сети связи и алгоритмов вычисления состояния ее компонентов;
– выработка множества допустимых вариантов (планов) построения СОТМ;
– выбор оптимального варианта (плана) по заданному критерию или множеству критериев;
– наращивание возможностей сети связи (если необходимо);
– построение СОТМ по выбранному плану (размещение и настройка компонентов СОТМ на узлах и настройка взаимодействия между компонентами);
– оценка качества функционирования СОТМ по заданному критерию.

Любая современная сеть связи потенциально динамична – как в структурном плане, так и в части парка применяемого оборудования. В связи с этим возникает необходимость адаптации СОТМ к подобным изменениям. Для СВ СОТМ такая адаптация по большей части (но не полностью) сводится к инициализации процедур ее МУФ. Процедура адаптации СОТМ также может быть инициирована по иным причинам, вследствие которых имеющаяся реализация СОТМ не отвечает в полной мере всем предъявляемым к ней требованиям.

Адаптация СВ СОТМ состоит из следующих основных этапов:

– анализ истории произошедших и плана ожидаемых изменений в сети связи с целью получения информации о новом составе узлов и направлений связи, а также наличии телекоммуникационных ресурсов, которые можно зарезервировать под СОТМ с новым качеством функционирования без ущерба качеству предоставляемых услуг связи;
– анализ изменений в сети с целью построения модели изменений предметной области;
– разработка комплекта компонентов метаинформации с описанием изменений в структуре сети связи и алгоритмах вычисления состояния ее компонентов;
– выработка множества допустимых вариантов (планов) адаптации СОТМ;
– выбор оптимального варианта (плана) по заданному критерию или множеству критериев;

– наращивание сети связи в интересах СОТМ (если необходимо);

– адаптация СОТМ по выбранному плану (перенастройка имеющихся компонентов СОТМ, размещение и настройка компонентов СОТМ на новых узлах и настройка взаимодействия между всеми компонентами);

– оценка качества функционирования СОТМ по заданному критерию после ее адаптации.

Наиболее важным моментом в первом и втором случае является то, что выработка планов (построения и адаптации соответственно) выполняется с учетом изначального (без СОТМ) состояния входящих в систему связи сетей связи, которые создавались для предоставления услуг связи: на качество предоставления этих услуг не должны повлиять изменения, связанные с построением и адаптацией СОТМ.

Предлагаемая методика за счет применения МУФ позволяет построить СОТМ, время и стоимость адаптации которой на порядок меньше, чем при традиционном подходе.

Панков Р.Н., Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОСНОВЫ ФОРМИРОВАНИЯ ПОЛЕВОЙ КОМПОНЕНТЫ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Современный этап развития систем связи характеризуется комплексным применением цифрового телекоммуникационного оборудования и сетевых технологий, позволяющим расширить возможности и повысить эффективность функционирования сетей связи. Система связи, выполняя задачи обеспечения информационного обмена в системе управления, должна быстро реагировать на изменения обстановки, динамично изменять свою структуру, с учетом построения системы управления и режимов её работы, обеспечивать должностных лиц пунктов управления современными услугами связи.

Полевая цифровая транспортная сеть связи (ТСС) должна обеспечить гарантированный обмен больших объёмов информации по стандартным (типовым) протоколам в зоне действий группировки войск (сил) между пунктами управления, как по каналам систем военной связи, так и с использованием ресурса единой сети электросвязи Российской Федерации.

Основу создаваемой перспективной полевой системы связи должна составить распределённая и равнодоступная для всех абонентов ТСС, являющаяся сетью связи общего пользования группировки войск (сил) в зоне ответственности. Это позволит исключить ее от громоздких и слабо защищённых от радиоэлектронного воздействия противника опорных узлов связи. Они должны быть заменены на узлы доступа, позволяющие инвариантно менять конфигурацию сети связи общего пользования в зависимости от обстановки и обеспечивающие доступ абонентов к ресурсу системы связи и услугам связи ЕСЭ России.

На современном этапе развития и уровне внедрения информационных и телекоммуникационных технологий в интересах системы связи группировки войск (сил) необходимо определить порядок построения распределённой и эшелонированной полевой транспортной сети связи, равнодоступной для предоставления ресурса абонентам, основу, которой должны составлять узлы доступа, имеющие в своём составе средства каналообразования для магистральных линий, линий связи привязки, линий прямой связи и сетей широкополосного доступа.

В дальнейшем по мере реализации инновационных проектов разработки и оснащением войск перспективными, помехоустойчивыми разведзащищенными цифровыми комплексами связи развитие системы связи специального назначения должно быть направлено на создание сетевой архитектуры и переход к принципу построения сетевой инфраструктуры.

Задачи формирования полевой компоненты ТСС заключается в том, чтобы для каждой последовательно выполняемой оперативной задачи по результатам прогнозируемой оценки воздействия противника на ТСС, определить потребность в полевой компоненте.

Исходные данными для определения потребности в полевой составляющей являются: количество выполняемых оперативных задач; местоположение узлов связи; поступающая в направления связи нагрузка; пропускные способности линий связи ТСС; характер возможного воздействия противника на ТСС.

Алгоритм определения потребности в полевой составляющей ТСС включает в себя задачи:

Оценка воздействия противника. При решении этой задачи необходимо определить прогнозируемое воздействия противника на узлы связи доступа ТСС, для чего произвести ранжирование узлов по категориям, внутри каждой категории по степени важности, с тем, чтобы спрогнозировать порядок воздействия противника на них. Следующим шагом необходимо произвести расчет разведзащищенности узлов связи транспортной сети, а для узлов связи находящихся в перечне вскрытых разведкой противника также рассчитать их живучесть.

Определения потребности в полевой составляющей. В этом блоке узлы связи, обладающие значением вероятности выживания менее порогового значения, будут считать гарантированно

пораженными противником. Эти узлы исключаются из ТСС, после чего осуществляется пересчет линий связи (определяются получившаяся структура транспортной сети связи).

Оценка структурной устойчивости ТСС, для этого определяется коэффициент связности ТСС, которая проводится с помощью алгоритма Клейтмана.

Оценка пропускной способности ТСС.В данном блоке проводится расчеты о оценки пропускной способности ТСС с учетом эшелонированной системы связи и технических средств с использованием которых она строиться.

Таким образом, на выходе методики определения потребности в полевой компоненте ТСС для каждого выполняемой оперативной задачи, получаются: таблицы недостающих значений пропускной способности направлений связи, матрица связности транспортной сети связи.

Выполнение алгоритма формирования заканчивается после того как получаются выходные данные для всех последовательно выполняемых в ходе операции оперативных задач, которые в свою очередь будут являться входными данными при формировании полевой составляющей ТСС в операции.

Паращук И.Б., Дедюрин А.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ GPGPU ДЛЯ ПРОИЗВЕДЕНИЯ НЕГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ

В настоящее время IT технологии прочно вошли во все сферы человеческой деятельности, некоторые из которых требуют больших вычислительных мощностей. Чаще всего нам необходимо оперативно получать результаты обработки (например, для обработки сейсмических данных или кодирования видео в режиме online). Для повышения производительности постоянно разрабатываются новые технологии и улучшаются характеристики оборудования. Одной из технологий является использование GPGPU.

С возрастанием возможностей компьютеров человечество находит им применения в прикладной и научной сфере деятельности. Особенно требовательны к аппаратным ресурсам такие задачи, как обработка и рендеринг потокового аудио-визуального контента высокого качества, моделирование физических процессов и явлений, обработка экспериментальных данных, воссоздание поведенческих особенностей и подражание мозговой деятельности. Обычному пользовательскому компьютеру с двух или четырехядерным CPU может понадобиться для таких расчетов несколько дней, а иногда недель или месяцев.

Для повышения производительности постоянно создаются новые технологии и аппаратное обеспечение. Создание технологий, позволяющих выполнять большое количество вычислений параллельно во множестве потоков дало хороший толчок к росту производительности.

GPGPU (General-purpose computing for graphics processing units) –техника использования графического процессора(GPU, англ. Graphics Pro-cessing Unit) видеокарты для выполнения не графических вычислений. Архитектура видеокарты позволяет быстро и без проблем “распараллелить” обработку данных, т.к. GPU обладает большим количеством ядер в отличие от CPU(англ. Central Processing Unit), что может затмить скорость вычислений даже самых мощных процессоров для многих параллельных задач обработки.

GPGPU используется для выполнения задач, которые раньше были прерогативой мощных процессоров, таких как шифрование/дешифрование, физические расчеты, научные вычисления, генерация криптовалют, таких как Bitcoin, финансовые расчеты, обработка сейсмических данных и тд.

Важный момент при использовании GPU заключается в том, что он реализует принцип SIMD(single instruction, multiple data- одиночный поток команд, множественный поток данных), принцип компьютерных вычислений, позволяющий обеспечить параллелизм на уровне данных.

Выполнение расчётов на GPU показывает отличные результаты в алгоритмах, использующих параллельную обработку данных. То есть, когда одну и ту же последовательность математических операций применяют к большому объёму данных.

При этом лучшие результаты достигаются, если отношение числа арифметических инструкций к числу обращений к памяти достаточно велико. Это предъявляет меньшие требования к управлению исполнением (flow control), а высокая плотность математических расчетов и большой объём данных отменяет необходимость в больших кэшах, как на CPU.

В отличие от последовательного выполнения команд друг за другом, производимых на центральном процессоре, графические процессоры оптимизированы для параллельного выполнения множества потоков.

Использование графических процессоров открывает большие возможности для вычислений и обработки большого количества информации. GPU не является заменой CPU, а скорее выполняет роль вычислительного блока и работает одновременно с ним.

Паращук И.Б., Царамов М.В., Сафонов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ОСНОВНЫХ ТРЕБОВАНИЙ К ПРОЦЕДУРАМ ПОИСКА И НАВИГАЦИИ В БОЛЬШИХ ОБЪЕМАХ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Не секрет, что проблема Больших Данных является актуальной и для региональных телекоммуникационных сетей (РТКС). Именно поэтому важное значение имеет процедура формулировки адекватных требований к поиску и навигации (ПиН) в больших объемах информации, циркулирующей в РТКС. Интерфейс систем ПиН в РТКС должен обеспечивать возможность единообразно организованного и оперативного поиска и навигации в больших объемах разнородной информации. Должна быть обеспечена техническая возможность полнотекстового поиска по содержимому баз данных (БД) РТКС.

Помимо этого, должны быть предъявлены требования к единым технических (программно-аппаратным) средствам ПиН по разнородным БД, обеспечивающим:

Навигацию во всем доступном информационном пространстве; наглядное предоставление пользователю логической структуры информационного пространства РТКС.

Лексический поиск (информационный поиск по лексике используемых в БД РТКС языков).

Символьный поиск – разновидность лексического поиска, где в качестве лексической единицы выступает определенная последовательность допустимых символов, например, даты.

Атрибутный поиск – информационный поиск объектов по значениям их характеристик.

Просмотр содержания информационного объекта и его структуры: последовательный (например, страница за страницей) и выборочный (переход на любую заданную страницу или на любой элемент, отраженный в структуре).

Многооконный режим работы, позволяющий пользователю одновременно видеть на экране два окна (как минимум) с разным содержанием. Одновременный вывод на экран (в разных окнах) текстов двух разных документов (файлов) или двух экземпляров одного документа.

Поддержка аппарата гипертекстовых и гипермедийных связей, обеспечивающего пользователю оперативный переход от документа к документу.

Протоколирование сеанса работы пользователя с возможностью перехода в любое из ранее существовавших состояний системы.

Выполнение пользователем настройки системы (задание определенной конфигурации окон, размеров шрифтов и др.).

Установка закладок в тексте информационных объектов и возможность оперативного перехода на них.

Экспорт информации из системы с указанием на источник (собственно электронный документ или БД и информационный объект, из которого копируется информация).

Списки, допускающие сортировку по значениям любого поля, определенного как ключевое.

Выполнение именно этих основных требования к процедурам поиска и навигации в больших объемах информации, циркулирующей в РТКС, позволяют надеяться на выполнение условий по своевременности, надежности и достоверности получения пользователями услуг, предусмотренных политикой построения и применения региональных телекоммуникационных сетей.

Паращук И.Б., Домбровский Я.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СУЩНОСТЬ ОБЕСПЕЧЕННОСТИ И УДОБСТВА ИСПОЛЬЗОВАНИЯ КАК КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ПРОЦЕССА ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Современные и перспективные региональные телекоммуникационные сети (РТКС), являясь принципиально новыми, гетерогенными и мультисервисными сетями, должны обеспечивать одновременное представление множества разнообразных услуг с требуемым качеством, выполнять запросы пользователей и оптимально использовать сетевой ресурс. Для анализа качества и эффективности функционирования сети в интересах оптимального управления ею, принято использовать системы показателей качества, причем традиционно рассматривают локальные системы показателей качества (ПК) более низкого уровня иерархии, которые характеризуют внутренние свойства сети, и глобальную систему ПК, описывающую внешние, пользовательские свойства РТКС. Это обусловлено реально существующим доминирующим значением одного процесса, протекающего в РТКС – процесса обслуживания пользователей, над другими процессами – информационного обмена, управления связью и сетевого мониторинга.

Основными внешними, пользовательскими свойствами гетерогенной и мультисервисной РТКС, характеризующими качество обслуживания, Quality of Service (QoS) – степень удовлетворения

пользователя предоставляемым ему обслуживанием, принято считать: обеспеченность обслуживания; удобство использования (прозрачность) услуг; действенность обслуживания, включающая доступность – временную доступность (своевременность) и топологическую доступность, непрерывность, целостность (достоверность); безопасность всего перечня телекоммуникационных услуг, оказываемых, потребителю определенного уровня иерархии.

При этом векторный ПК обеспеченности обслуживания должен количественно характеризовать объем и номенклатуру предоставляемых пользователю (определенного уровня иерархии) услуг РТКС. Данный вектор характеризует возможность РТКС предоставлять пользователям такое количество определенного вида услуг (из всего допустимого множества видов услуг, предоставляемых РТКС), которое соответствует потребностям абонентов и задачам сети в конкретный момент времени.

Вектор показателей удобства использования услуг должен описывать способность (свойство) РТКС и включать параметры, численно характеризующие, насколько успешно и легко потребитель может воспользоваться данными услугами сети. Рассмотрим данные свойства. Удобство использования услуг (обслуживания) зависит от трудоемкости выполняемых пользователем операций в процессе доступа и пользования полученной услугой и может быть описано с помощью объема команд (знаний) пользователя, необходимых для получения услуг и объема вводимой информации (знаков) с клавиатуры терминала РТКС в процессе доступа и пользования услугами. Значение этих параметров должно быть минимальным.

Помимо этого, при описании удобства обслуживания с точки зрения минимизации знаний потребителя о месте расположения программных и аппаратных ресурсов РТКС, о синтаксисе команд, о форматах пакетов технологий связи и т.д., можно и нужно говорить о прозрачности сети, которая достигается в том случае, когда сеть представляется пользователям не как множество отдельных терминалов и коммутаторов, связанных между собой сложной системой интерфейсов и кабелей, а как единое технико-технологическое устройство (например, ЭВМ) с системой разделения времени. Прозрачность означает, что пользователь для работы с удаленными ресурсами РТКС использует те же команды и привычные ему процедуры, что и для работы с локальными ресурсами РТКС.

Паращук И.Б., Гнедь Е.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПОДХОД К ФОРМУЛИРОВКЕ ПОКАЗАТЕЛЕЙ ДЕЙСТВЕННОСТИ ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ РЕГИОНАЛЬНЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Одним из внешних, пользовательских свойств региональных систем хранения данных (РСХД) и региональных телекоммуникационных сетей (РТКС), характеризующих степень удовлетворения пользователя предоставляемым ему обслуживанием, принято считать действенность обслуживания пользователей. Этот термин имеет множество толкований, мы предлагаем считать, что действенность обслуживания пользователей РСХД и РТКС – векторный показатель, включающий доступность (временную доступность (своевременность) и топологическую доступность), непрерывность и целостность (достоверность).

Иными словами, векторный показатель качества (ПК) действенности обслуживания пользователей является одним из важнейших в структуре показателей качества обслуживания, а входящие в него показатели призваны количественно описывать способность (свойство) РСХД и РТКС: предоставлять услуги пользователям тогда, когда это им необходимо; в необходимом пользователям месте; и в течение требуемого времени (продолжительность предоставления услуг) с требуемым качеством (достоверность и целостность предоставления услуг).

При этом векторный ПК доступности обслуживания РСХД и РТКС включает элементы, которые характеризуют свойство обслуживания быть предоставленным пользователю тогда и там, когда и где это ему необходимо. Он включает временную компоненту (когда, своевременность) и топологическую компоненту (где).

Векторный показатель доступности обслуживания, характеризующий свойство обслуживания быть предоставленным пользователю тогда и там, когда и где это ему необходимо, включает: вектор показателей временной доступности, характеризующий способность РСХД и РТКС обеспечивать доступ, например, подвижных абонентов, к ресурсам сети и предоставление им требуемого перечня услуг в установленные сроки (своевременность предоставления пользователям услуг); вектор показателей топологической доступности, характеризующий способность РСХД и РТКС обеспечивать доступ абонентов к ресурсам системы хранения (сети) и предоставление им требуемого перечня услуг в установленном месте их нахождения и при смене местонахождения абонента (при перемещении пользователя).

Элементы вектора показателей непрерывности обслуживания пользователей РСХД и РТКС характеризуют свойство обслуживания, будучи предоставленным, продолжаться в течение требуемого времени.

Вектор показателей целостности обслуживания пользователей РСХД и РТКС также, как и вектор показателей непрерывности, входит в состав одного из векторных показателей QoS – векторного показателя действенности обслуживания, а показатели, входящие в этот вектор, численно характеризуют точность, достоверность и полноту обслуживания, а также защищенность обслуживания (передаваемой и принимаемой информации) от возможных непреднамеренных и злоумышленных искажений.

Таким образом, подводя итоги процесса формулировки компонент вектора показателей действенности обслуживания пользователей РСХД и РТКС, отметим, что он содержит три составляющие – вектор показателей доступности обслуживания, включающий элементы (параметры, показатели) временной и топологической доступности; вектор показателей непрерывности обслуживания пользователей и вектор показателей целостности обслуживания пользователей, включающий элементы (параметры, показатели) достоверности и неискаженности.

Паращук И.Б., Михайличенко Н.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

НЕЙРО-НЕЧЕТКИЕ МОДЕЛИ В ИНТЕРЕСАХ УПРАВЛЕНИЯ ДАННЫМИ В ЦОД И ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ИНФОРМАЦИИ В РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В современных системах управления большими техническими системами все чаще используются сложные интеллектуальные методы и системы анализа данных. Рассмотрим некоторые современные подходы, способные повысить эффективность управления данными в центрах обработки данных (цод) и в региональных телекоммуникационных сетях (РТКС).

В последние годы в этом качестве все чаще находят применение нейро-нечеткие сети (системы) - системы анализа данных, совместно использующие нейросетевые структуры и нечеткую логику для управления сложными динамическими объектами в условиях неопределенности.

Иногда их используют как экспертные системы и называют нейро-экспертными. Они представляют собой нейро-нечеткую сеть (ННС), соответствующую некоторой определенной нечеткой модели вывода, причем знания экспертов (априорный опыт системы) в форме лингвистических переменных и нечетких правил логического вывода могут быть взаимно и однозначно отражены в структуре нейро-нечеткой сети.

Иными словами, включение концепции нечеткой логики в нейронные сети – формирование нейро-нечеткой сети, дает возможность такой гибридной системе иметь дело с «человекоподобным процессом рассуждений», закладывать в базу знаний (информационное поле) искусственной нейронной сети (ИНС) априорный опыт экспертов, использовать нечеткое представление информации, извлекать знания из входного потока показателей. Объединение возможностей нейронных сетей и нечеткой логики является наиболее перспективным подходом к организации современных систем интеллектуального анализа данных любой природы.

Нейро-нечеткие сети могут быть реализованы несколькими методами (способами). В простейшем случае это, так называемая, совместную модель ННС – ее можно рассматривать, как препроцессор, где механизм обучения ИНС (ANN – Artificial Neural Network) определяет правила нечеткого интерфейса СНВ (FIS – Fuzzy Inference System). Как только параметры СНВ определяются, ИНС работает в обычном режиме. Функции принадлежности обычно аппроксимируются нейронной сетью из обучающих данных.

Другой подход в реализации нейро-нечетких моделей в интересах управления данными в ЦОД и интеллектуального анализа информации в РТКС – это параллельная модель, в которой нейронная сеть помогает нечеткой системе определить требующиеся параметры, особенно если входные переменные системы не могут быть непосредственно измерены. Обучение происходит только в нейронной сети и нечеткая система остается неизменной. В некоторых случаях нечеткие выходы не могут быть непосредственно применены к процессу. В этом случае нейронная сеть может действовать как постпроцессор нечетких выходов.

Параллельная нейро-нечеткая модель, в которой входные данные подаются на нейронную сеть, а выход из нейронной сети дополнительно обрабатывается с помощью нечеткой системы.

Важной особенностью нейро-нечетких сетей является способность автоматически генерировать систему нечетких правил, извлекая скрытые закономерности изданных обучающей выборки.

Выбор нейро-нечетких моделей (совместных либо параллельных) осуществляется в зависимости от класса реально решаемых задач управления данными в ЦОД и интеллектуального анализа информации в РТКС.

Подниколенко А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ MPLS-TP В ТРАНСПОРТНЫХ СЕТЯХ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ

Современные вооруженные конфликты характеризуются скоротечностью проводимых операций, успех или поражение которых зависит от времени реакции системы управления войсками на изменение обстановки в значительно большей степени, чем в войнах проводимых ранее, что требует от Вооруженных Сил Российской Федерации совершенствования систем военной связи.

Внедрение в военные системы связи технологий пакетных транспортных сетей позволит учесть новые требования к сетевой инфраструктуре систем в части предоставления новых широкополосных пакетных приложений и сервисов и повысить оперативность управления войсками в условиях высокой динамики ведения боевых действий. На сегодняшний день и в ближайшей перспективе одним из лучших решений NGN является технология MPLS-TP, обладающая максимальной гибкостью и способствующая повышению эффективности функционирования сети.

Технология MPLS (Multi-Protocol Label Switching) ориентирована на быструю коммутацию на уровне звена данных, передачу пакетного трафика IP, обеспечение качества обслуживания QoS, масштабируемость сети, оптимизацию распределения трафика и эффективную маршрутизацию в соответствии с требованиями сетей NGN. Главная особенность технологии MPLS – отделение процесса коммутации пакета от анализа IP-адреса в его заголовке, что позволяет осуществлять коммутацию пакетов значительно быстрее.

Основная польза от технологии MPLS состоит в том, что она создает основу для развертывания новых типов услуг, не поддерживаемых традиционной маршрутизацией. Одновременно MPLS позволяет уменьшить себестоимость и улучшить качество базовых услуг и расширить возможности маршрутизации, позволяя учитывать многие факторы (а не только адрес назначения пакета). При внедрении нового типа услуг, ему нет необходимости заменять всю MPLS-совместимую инфраструктуру, достаточно всего лишь изменить управляющую составляющую. В настоящее время MPLS является ведущей технологией способной стать фундаментом для инфраструктуры мультисервисных сетей следующего поколения NGN, в рамках которых станет возможна передача любого трафика через единую телекоммуникационную инфраструктуру.

Однако, при всех достоинствах применения протокола MPLS, он до сих пор имеет определенные проблемы с масштабированием и междоменным взаимодействием, а также сохраняются проблемы сквозного (точка-точка) управления производительностью и качеством обслуживания (QoS), особенно в средах разных производителей. Поэтому необходимо применять более гибкие и современные решения, начиная от NGSDH и OTN, и заканчивая T-MPLS, PBT/PBB-TE и MPLS-TP.

Сеть на основе MPLS-TP имеет все преимущества IP/MPLS, но проще в эксплуатации и настройке, дешевле, чем классическая MPLS, и ориентирована решение задач уровня транспортных сетей. Кроме этого позволяет осуществлять интеллектуальное и динамическое управление сетью, в том числе динамического перераспределения канального ресурса сети.

Из выше сказанного следует, что внедрение технологии MPLS-TP в военную систему связи позволит значительно усовершенствовать методы решения задач управления войсками, более успешно решать вопросы, связанные с динамическим управлением канальным ресурсом сети, его эффективным использованием, обеспечением сетевых защитных механизмов коммутации, передачей новых инфокоммуникационных услуг и упрощением архитектуры сети.

В практической части статьи рассмотрено применение магистрального MPLS-TP маршрутизатора 1850 TSS-320 компании Alcatel-Lucent, совместимого с учебной телекоммуникационной сетью ВАС.

Полугина Ю.К.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МЕТОДЫ ОЦЕНКИ КАЧЕСТВА VOIP СВЯЗИ

IP телефония, как пакетная технология, не гарантирует высокого качества передачи данных, особенно в условиях повышенной нагрузки. Оценить качество звучания можно субъективным способом – собеседника достаточно четко, громко слышно, отсутствуют долгие задержки и эхо. Объективный способ предполагает учитывать число доставленных и потерянных пакетов, а также скорость их передачи. Но в случае с VOIP наличие лишь объективного метода оценки качества не раскрывает цельной картины, поэтому официально рекомендуемым способом оценки качества IP и других типов речевой связи является усредненная субъективная оценка MOS (Mean Opinion Score), алгоритм определения которой был описан в Рекомендациях ITU-T P.800 и P.830. Она формируется на основе большого числа испытаний, в каждом из которых участвует множество экспертов. Возможные значения MOS находятся в пределах от 1 до 5. Средний показатель с цифрой 4

соответствует хорошему качеству речевого соединения, менее 3,5 означает неудовлетворительное качество.

Другим субъективным методом оценки качества является использование единиц рейтинга R (Quality Raiting) по стобалльной шкале, где R=100 по стандартам ITU-T соответствует высшему качеству и MOS=4,5.

Недостатками указанных способов измерения качества передачи речи являются их субъективность и неэффективность их использования ежедневно на практике, т.к. они не учитывают изменение и появление различных факторов в сети, таких как нагрузка, например. Поэтому возникают попытки автоматизировать процесс оценки.

Первым автоматизированным алгоритмом оценки стал PSQM (Perceptual Speech Quality Measure), который утвердили в подразделении Международного союза электросвязи (ITU-T) и уже используют в некоторых системах. Принцип работы алгоритма предполагает передачу по VoIP-сети специальных речевых шаблонов и сравнение полученной информации на принимающей стороне. Единственный недостаток этого алгоритма был устранен в другой модификации - PESQ (Perceptual Evaluation of Speech Quality), который теперь учитывает флуктуацию задержки (или джиттер).

В 2003 году специалисты международной организации ITU-T, совместно с компаниями Psytechnics, Opticom и SwissQual сравнивали результаты измерения качества передачи речевой информации, полученные по алгоритму PESQ, с экспертными оценками MOS, предоставленными компаниями AT&T и BT. Корреляция между двумя группами оценок, составила 0,95 — очень хороший результат. И позже ITU-T одобрил алгоритм PESQ в качестве стандарта. PESQ, который рассматривают в качестве преемника PSQM, более точно измеряет качество телефонной связи через IP-сети, учитывает влияние нагрузки на сеть, т.е. задержки пакетов.

С другой стороны, недостатком PESQ является то, что они основываются на сравнении аудиопотоков на входе и выходе системы. Это так называемый мониторинг методом «активного тестирования». Но такой способ дополнительно нагружает сеть лишним трафиком, что влечет некоторые проблемы в ходе тестирования.

Поэтому пока самым лучшим способом определения качества связи в сетях VoIP считается оценка его самими абонентами. Степень вредного воздействия шума, эха, задержек или помех на качество речевой связи определяется тем, насколько они комфортно могут в это время разговаривать конкретные абоненты В. теории, для точной оценки следовало бы регулярно проводить опросы достаточно большого числа абонентов на предмет удовлетворенности связью, поскольку восприятие качества речевой связи всегда субъективно. Однако, на практике это просто не осуществимо. К тому же появление и исчезновение нагрузки происходит чаще всего незапланированно, среагировать на изменение достаточно быстро невозможно.

Кроме того, нужно иметь в виду, что оценка степени удовлетворенности абонентов – очень сложный и субъективный показатель. Его сложно определить его количественно и точно, сложнее, чем просто померить скорость загрузки страницы или доставки письма. Именно поэтому совершенствование автоматизированных способов оценки качества связи является достаточно актуальной задачей оптимизации VOIP связи.

Присяжнюк С.П., Зализнюк А.Н.
Россия, Санкт-Петербург, АО Институт телекоммуникаций
г. Москва, Военно-топографического управления Генерального штаба Вооруженных Сил РФ

НАПРАВЛЕНИЯ РАЗВИТИЯ СТРАТЕГИЧЕСКОГОГО ПЛАНИРОВАНИЯ ГЕОИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СИСТЕМ УПРАВЛЕНИЯ

Функционирование современными сложными организационными системами управления территориями (СУТ) требует постепенного и своевременного геоинформационного обеспечения.

В условиях повышения требований, начавшейся четвертой индустриальной революции с широким использованием искусственного интеллекта и когнитивных информационно-управляющих систем, на эффективность процесса геоинформационного обеспечения влияет качество планирования, которое является основополагающей стадией принятия решений о будущем состоянии геоинформационного обеспечения.

Характерной особенностью геоинформационного обеспечения СУТ, является то, что обеспечения необходимо на разные районы территории с различающимися требованиями с особенностями.

В этих условиях цель геоинформационного обеспечения СУТ заключается в своевременном изготовлении требуемых объектов геоинформационной продукции, инфраструктуры и ее обеспечения с заданным качеством на каждом этапе планирования и за весь период в целом.

Предлагается метод стратегического планирования, геоинформационного обеспечения систем управления регионами и его инфраструктурой. Суть метода заключается в поиске оптимального плана при ограниченном ресурсе, максимально увеличивающий количество своевременного изготовленных качественно унифицированных геоинформационных продуктов в интересах СУТ.

Для решения поставленной задачи рассматривается случай, в условиях, когда спрос формируется в виде совокупности районов с различным количеством унифицированной геоинформационной продукции в каждом районе и в условиях перегрузки, когда спрос превышает возможности.

Разработаны принципы успешного планирования при ограниченном ресурсе путем расстановки динамических приоритетов унифицированным геоинформационными продуктами при которых обеспечивается максимум производительности.

Процессы тактического, перспективного и стратегического планирования становится единым непрерывным процессом с возможностью оперативной коррекции планов в условиях непредвиденного изменения внешней среды.

Применение динамических приоритетов позволяет автоматизировать процесс планирования с реализацией принципов непрерывности, гибкости, точности, единства и участия всех заинтересованных сторон с целью обеспечения сбалансированности совместной работы.

Разинов А.А., Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРЕДЛОЖЕНИЯ ПО СОСТАВУ ПРОГРАММНО- ТЕХНИЧЕСКОГО КОМПЛЕКСА ОРГАНОВ УПРАВЛЕНИЯ СВЯЗЬЮ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИИ

Для обеспечения управления войсками и силами в органах управления связью необходимо разработать программно-технический комплекс (ПТК) автоматизированных рабочих мест (АРМ) должностных лиц (ДЛ) органов управления связью (ОУС) и автоматизацией управления войсками (АУВ).

Исходя, из решаемых задач должностными лицами ОУС ПТК установленный на АРМ должен обеспечить:

- информационную поддержку ДЛ ОУС и АУВ ФС ВНГ РФ и в их повседневной деятельности, и при выполнении учебно-боевых задач;
- повышения оперативности управления системой связи и АУВ за счет применения средств автоматизации;
- формирование единого информационного пространства в звене: ГК ВНГ РК – соединений органов управления связью и АУВ ФС ВНГ РФ;
- повышение эффективности и интенсификация внутриведомственного обмена информацией органов управления связью и АУВ.

Для функционирования АРМ должны использоваться штатные технические средства автоматизации (персональные компьютеры – рабочие станции) ДЛ ОУС и АУВ ФС ВНГ РФ.

ПТК АРМ ДЛ ОУС и АУВ должен функционировать в единой ЛВС ФС ВНГ РФ под управлением операционных систем – MS Windows 7/8.1 (для РМ); MS Windows 2012 server R2.

Система управления базами данных (СУБД) - MS SQL server 2012. Должен быть совместим с ГИС «Гармония». ПТК АРМ ДЛ ОУС и АУВ должен включать:

а) комплекс технических средств (КТС);

б) общее программное обеспечение (ОПО):

- операционную систему (ОС);
- систему управления базами данных (СУБД);
- геоинформационную систему (ГИС);

в) специальное программное обеспечение (СПО) АРМ ДЛ ОУС и АУВ:

программные компоненты, согласно решаемым задачам ДЛ ОУС и АУВ;

г) комплект эксплуатационной документации (ЭД).

ПТК АРМ ДЛ ОУС и АУВ должен содержать следующие программные компоненты:

Программные компоненты должны функционировать в едином информационном пространстве, обеспечиваемом центральной базой данных (БД), входящей в состав информационного обеспечения ПТК АРМ ОУС и АУВ.

ПТК АРМ ОУС и АУВ должен предусматривать:

- средства контроля целостности, корректности и непротиворечивости данных;
- резервное копирование (архивация) данных, а также возможность настройки сессий автоматического копирования, которые должны быть предусмотрены стандартными функциями системы управления базами данных и имеющегося программного обеспечения сервера баз данных;
- средства печати документов.

Программное обеспечение (ПО) АРМ должно обеспечивать расширение состава реализуемых функций путем модификации и (или) замены установленным порядком программного обеспечения в процессе эксплуатации, обеспечивать адаптивность к изменению состава ПТК АРМ в согласованном объёме требований, обеспечивать автоматизированное полное и (или) частичное информационное восстановление после отказа и иметь модульную структуру;

ПО должно быть детально документированным и обеспечивать необходимый и достаточный для реализации основных функций набор АРМ, выделенных по функционально-технологическому принципу;

ПО должно обеспечивать пользовательский интерфейс на русском языке.

Разработка и применение представленного статье комплекса позволит должностных лицам органов управления связью ВВ МВД осуществляю управление в автоматизированном режиме и значительно сократиться время на принятие решения.

Репников А.Ю., Пустошкин М.М., Худайназаров Ю.К.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПЕРЕСЕКТИВЫ РАЗВИТИЯ СРЕДСТВ РАДИОМОНИТОРИНГА

Проблема обеспечения, автоматизированного радиомониторинга (далее – АРМ) и радиоконтроля, в настоящее время связана с постоянным возрастанием количества угроз безопасности информации со стороны спецслужб зарубежных стран, которые осуществляют сбор сведений о промышленных и экономических секретах российских предприятий и ведут контроль за научными и техническими разработками во всех областях, связанных с перспективными технологиями.

В качестве обобщенного показателя оценки средств АРМ наиболее подходит критерий «эффективность – стоимость», при этом эффективность средства лучше всего характеризует вероятность выполнения соответствующей задачи радиомониторинга за фиксированный интервал времени при условии наличия исходных данных.

Сегодня основные тенденции (направления) развития средств и методов радиомониторинга определяются двумя факторами.

Первый фактор определяет необходимость решения задач по управлению использованием радиочастотного спектра.

Второй фактор – необходимость соответствия уровня методологии и технической оснащенности систем радиомониторинга уровню развития средств связи.

Наряду с многочисленными радиотехнологиями большое внимание уделяется перспективным радиотехнологиям, находящимся на стадии внедрения (становления), к которым можно отнести следующие:

- цифровая сотовая связь IMT-2000 (UMTS/W-CDMA);
- радиотехнологии широкополосного радиодоступа.

К числу наиболее распространенных характерных признаков классификации технических средств радиомониторинга можно отнести:

- размеры зоны радиодоступности;
- функциональное назначение;
- характер использования;
- продуктивность оборудования;
- особенности конструктивного исполнения.

При этом такое разделение является достаточно условным. Все большей популярностью в последнее время пользуются автоматизированные системы, в которых удаленные станции, функционируя в автоматизированном режиме, выполняют расширенный объем задач — от выявления радиоизлучений до автоматической проверки соответствия их параметров заданным значениям («маске» сигналов) и представляют собой радиочастотные сенсоры (датчики).

На практике основная нагрузка в решении задач радиомониторинга ложится на подвижные (мобильные) станции. В дополнение к стационарной компоненте подвижные станции представляют собой гибкое средство обеспечения контроля за использованием РЧС, особенно подходящее для проведения измерений вблизи передатчиков, которые характеризуются, например, низким уровнем мощности, высокой рабочей частотой, узкими диаграммами направленности антенных систем и т.д.

Мобильные станции могут быть интегрированы в стационарные сети (с использованием каналов передачи данных систем сотовой связи) в качестве дополнительных СРМ с целью временного расширения зоны радиодоступности РПРМ. В результате такой интеграции СРМ получает уникальную возможность, помимо расширения зоны радиодоступности стационарной компоненты, также использовать мобильные станции, оснащенные системами радиопеленгования, для уточнения координат ИРИ, а МСРМ - для оперативных заданий по проведению радиоконтроля. Во многих случаях задачи контроля из-за трудностей определения местонахождения РЭС могут быть эффективно решены только при использовании мобильных средств, применяемых в дополнение к стационарным СРМ.

Построение распределенных систем сбора данных возможно на базе современных сетей сотовой связи и «умных» мобильных телефонов, операционные системы которых имею множество

уязвимостей. Известные технологии программно-определяемых сетей (SDN) используются для построения наложенных сетей на базе сетей крупных операторов связи.

Таки образом, актуальной задачей является разработка масштабируемой распределенной системы радиомониторинга в составе мобильных станций и радиочастотных сенсоров-сигнализаторов с возможностью контроля сетей сотовой связи и широкополосного доступа. Предлагаемая структура такой системы состоит из:

1. Мобильных обслуживаемых средств радиомониторинга, интегрируемых в стационарные сети радиомониторинга.

2. Дистанционно управляемых автономных датчиков, интегрируемых в стационарные сети связи, полевые аппаратные связи, размещаемых на беспилотных летательных аппаратах.

Сабуров А.В., Крючков Д.В., Бегмахмудов И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МЕТОДЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ПЕРЕДАЧИ РЕЧЕВЫХ СООБЩЕНИЙ С КОММУТАЦИЕЙ ПАКЕТОВ ПО IP-СЕТЯМ

В настоящее время на основе достижений в области современных цифровых технологий продолжается процесс конвергенции и интеграции компьютерных и телекоммуникационных сетей, т.е. процесс объединения систем связи и автоматизированных систем управления (АСУ) в единую информационно-телекоммуникационную систему, включающую в себя информационную, телекоммуникационную и организационную составляющие. Практически всех операторов в развитии электросвязи привлекает интегрированный способ передачи единой телекоммуникационной сетью любого вида услуг: речи, данных, видео и пр. Используя новые технологии и, в частности, коммутацию пакетов (КП), можно технически решить поставленную задачу. В последнее время основное внимание мира телекоммуникаций приковано к технологиям передачи речевой информации с коммутацией пакетов, в частности, по IP-сетям. Такой способ передачи речи получил название IP-телефония. Речевая информация относится к трафику реального времени, соответственно проблемы задержки и потери пакетов в процессе передачи речи по IP-сети являются серьезной проблемой с точки зрения обеспечения приемлемого качества оказания услуг IP-телефонии. В данной статье мы рассмотрим методы обеспечения качества передачи речевых сообщений с коммутацией пакетов по IP-сетям и проведем краткий анализ технологий.

Протокол RSVP (Resource ReSerVation Protocol) применяется для резервирования сетевых ресурсов. В результате, по всему пути от абонента до абонента резервируется необходимая пропускная способность с целью обеспечения запрашиваемого качества обслуживания.

Протокол RTP (Real-time Transport Protocol) - для компенсации негативного влияния вариации задержки. Протокол переносит в своем заголовке данные, необходимые для восстановления, в частности, аудиоданных в приемном узле, временную метку и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты.

RTCP (Real-time Transport Control Protocol) - для контроля доставки RTP-пакетов и обеспечения связи с передающей стороной.

Механизм дифференцированного обслуживания (одна из моделей QoS) используется для классификации потоков в соответствии с предопределенными правилами и дальнейшего объединения однотипных потоков.

Назначение MPLS сходно с назначением дифференцированного обслуживания, но помимо этого MPLS позволяет значительно сократить время на обработку маршрутной информации в узлах сети и, следовательно, уменьшить задержку сигнала.

Протокол IPv6 (Internet Protocol version 6) - новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4).

Протокол IPv6 обладает рядом преимуществ:

- расширенное адресное пространство (делает NAT необязательным, что упрощает маршрутизацию);
- убраны функции, усложняющие работу маршрутизаторов;
- появились метки потоков и классы трафика;
- реализована функция автоконфигурации посредством обмена ICMPv6 пакетами.

Фактически IP – это архитектура, предполагающая системный подход к построению сетей передачи данных, на базе которых возможно было бы предоставлять современные услуги с применением новейших технологий, а также удовлетворяющих целому ряду условий и требований. Однако нужно понимать: это, в первую очередь, всего лишь концептуальный подход к построению современных сетей уровня оператора связи, позволяющий оптимальным образом реализовать все преимущества используемых технологий, приложений и ресурсов, обеспечивая оператору конкурентное преимущество, оптимизацию расходов. В настоящее время в международных

организациях и форумах идет непрерывная разработка новых стандартов и протоколов, связанных с передачей речи по сетям с пакетной коммутацией. Производители аппаратного и программного обеспечения регулярно представляют на рынок свои новые продукты. Иными словами, IP-телефония, безусловно, перешла из разряда перспективной технологии в реальную альтернативу традиционной телефонии, заняв свою нишу на телекоммуникационном рынке.

Таким образом мы считаем, что наш анализ методов обеспечения качества передачи речевых сообщений с коммутацией пакетов по IP-сетям принесут пользу в понимании функционирования и построения транспортных сетей на основе IP - передачи пакетных речевых сообщений.

Савенков С.Н., Ногин С.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ВИРТУАЛИЗАЦИЯ ОБРАБОТКИ ДАННЫХ

Необходимость развертывания учебных фрагментов АСУ при проведении занятий по оперативной и технической подготовке. Использование IaaS предполагает 2 этапа:

1. Подготовка
2. Применение.

На первом этапе готовится инфраструктура виртуальной АСУ.

На втором этапе готовая инфраструктура адаптируется под цели занятия и требования пользователей.

1. Подготовка.

– Развертывание в центре обработки данных пункта управления системы виртуализации «Nebula».
– Создание АРМ должностных лиц на базе виртуальных машин (клонирование).
– Создание сервера функциональной группы на базе виртуальной машины.
– Настройка сервера функциональной группы.
– Создание сервера комплекса средств автоматизации на базе виртуальных машин.
– Настройка сервера КСА.
– Создание инфраструктуры функциональной группы.
– Настройка доменной структуры (адреса, разграничение доступа (роли) стандартными средствами АСУ)
– Организация системы защиты информации в домене.
– Клонирование виртуальной инфраструктуры домена.
– Создание дерева доменов.
– Архивирование инфраструктуры.

2. Применение

– Анализ требований пользователей к вычислительной инфраструктуре для проведения мероприятий оперативной подготовки (занятий). (Количество доменов, количество АРМ, типы серверов, требуемые ресурсы, используемое программное обеспечение).
– Развертывание виртуальной инфраструктуры в соответствии с требованиями пользователей.
– Настройка виртуальной инфраструктуры (адреса, роли, назначение прав доступа).
– Предоставление услуги.

Достоинства

– Повторяет структуру системы управления.
– Сокращение общего времени на развертывание учебного фрагмента.
– Структура системы легко меняется путем наращивания или уменьшения числа доменов или АРМ в функциональной группе в зависимости от поставленных целей обучения
– Не требует дополнительных технических и программных средств на развертывание учебных фрагментов.
– Пользователи могут работать со своих рабочих мест.
– Функции администратора (внутри фрагмента) сводятся к предоставлению доступа к ресурсам.
– Быстрое восстановление информационного процесса при выходе из строя элементов учебного фрагмента.

Недостатки:

– Повышенные требования к ресурсам внешней системы (вычислительная мощность, большой объем оперативной и внешней памяти).
– Сложность внешнего администрирования (работа с облачными технологиями).

Сазонов В.В., Арсентьев А.И., Мосягин Д.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СЕТИ РАДИОСВЯЗИ

Известно, что для повышения эффективности деятельности должностных лиц, органов управления связью при решении задач по радиосвязи в условиях повышения технологической сложности её элементов, предопределило наращивание «глубины» автоматизации сети радиосвязи в основном на технологическом уровне. Это привело к развитию функций управления телекоммуникационным оборудованием и мониторинга, а с другой стороны – к необходимости применения проприетарных протоколов управления заложенных в комплексы радиосвязи различных производителей.

Оперативное подключение/отключение отдельных комплексов радиосвязи в процессе ведения сеанса связи изменяют её структуру, что приводит к усложнению закладываемых протоколов. В таких комплексах радиосвязи автоматически осуществляется идентификация текущего состояния телекоммуникационного оборудования и каналов взаимодействия, динамической маршрутизацией доставки данных. Физические каналы обмена данными поддерживаются аппаратурной частью комплексов радиосвязи, а всё остальное реализуется программно. В основу программного обеспечения комплексов радиосвязи закладывается сетевая модель комплекса радиосвязи, в которой отражены все существующие детали сетевого взаимодействия. В каждом транзитном и оконечном комплексе сеть радиосвязи представлена программным модулем, который должен поддерживать группу проприетарных протоколов управления, заложенными в сетевую модель для этого комплекса. Модель задаётся базами данных и динамическими правилами их преобразования.

Анализируя каталоги более шестидесяти предприятий промышленности в области связи, можно сказать, что почти половина имеет предложения по поставкам и услугам построенных на сетях радиосвязи. Продукция выпускаемая данными предприятиями характеризуется высокой мобильностью, устойчивостью, крипто- и помехозащиты. Создаваемые программно-аппаратные платформы уже используют отечественную элементную базу, например ОАО «НПО Ангстрем». Так же предусмотрены возможности использования различных технологий связи, современных сигнально-кодовых конструкций и сигналов унаследованных сетей радиосвязи, криптографической защиты информации и программного обновления комплексов.

Однако, имея огромный выбор системотехнических и технологических решений, задача разработки проприетарных протоколов управления остается открытой.

Сазонов В.В., Титов В.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРЕДЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СИСТЕМ ДОКУМЕНТАЛЬНОГО ОБМЕНА

Сети документального обмена военного назначения обеспечивают своевременную, достоверную и скрытую передачу документов по управлению войсками, отчетно-информационных и справочных документов.

К документам по управлению войсками относятся решения, планы, боевые приказы, распоряжения и оперативные директивы, распоряжения по различным видам обеспечения, рабочие карты и т.п. Отчетно-информационными документами являются боевые донесения, оперативные и разведывательные сводки, донесения и сводки по видам обеспечения (в том числе по связи, тылу и т.д.), отчеты, журналы боевых действий, схемы). В справочных документах содержатся результаты оперативных расчетов и математического моделирования боевых действий, ведомости боевого состава войск, другие справочные материалы для работы органов военного управления.

Вид и форма представления документов определяется соответствующими руководствами и наставлениями, а также используемыми оконечными и коммутационными средствами, с помощью которых осуществляется ввод-вывод, обработка и передача документов по соответствующим сетям.

Оконечные средства, в зависимости от метода преобразования информации, могут быть двух основных видов: кодовые и факсимильные.

К кодовым средствам можно отнести телеграфные аппараты типа П-115 и П-116, различные абонентские телеграфные установки (удаленные и местные), абонентские пункты (низкоскоростные АП-Н и среднескоростные АП-С), позволяющие вести автоматизированный документальный обмен по протоколам АСДО «Экватор», комплекс технических средств обработки сообщений, автоматизированной сети открытой телеграфной связи на базе ЦКС СТИН-Э, автоматизированные абонентские телеграфные терминалы типа АТТ-4У и ПЭВМ с оконечным периферийным оборудованием в виде клавиатуры, принтера или алфавитно-цифрового печатающего устройства.

Рассмотренные разнородные кодовые оконечные и коммутационные средства не позволяют обеспечить их информационное сопряжение между собой как по форматам, так и по протоколам обмена телеграфными сообщениями.

Дополнительно следует отметить, что ряд решений по организационно-техническому построению сетей телеграфной связи морально устарел, а их пропускная способность не обеспечивает современных потребностей документального обмена. Применение средств телеграфной связи пока оправдывается лишь отлаженной станционно-эксплуатационной службой на телеграфных центрах узлов связи пунктов управления ВС РФ.

Факсимильный способ передачи обеспечивает более высокое соответствие принятой копии оригиналу, а также исключает значительную часть ошибок обслуживающего персонала за счет автоматизации процессов ввода, обработки, передачи-приема и выдачи копии документа пользователю. В сетях факсимильной связи для съема с носителя и нанесения информации на носитель используются факсимильные аппараты П-111 и П-112, принятые на вооружение. Кроме того, возможно использование специальных средств обмена цветной и одноцветной графической информацией с использованием графических редакторов «Равелин», ГИС «Интеграция» и «Рокада».

В связи с внедрением новых информационных и телекоммуникационных технологий в ВС РФ настоящее время развернуты и широко используются системы автоматизированного документооборота в электронном виде, которые предоставляют услуги электронной почты. К ним можно отнести межвидовую систему обмена электронной корреспонденцией, закрытый сегмент сети передачи данных, различные информационно-расчетные системы существующих АСУВ.

В полевых условиях документальный обмен возможен с применением комплекса технических средств обработки сообщений (КТС ОС) из состава комплексных аппаратных (КАС) типа П-260-О, а также КАС типа П-240И, П-240И-4, МП-2ИМ, в которых дополнительно предусмотрена установка абонентского телеграфного терминала АТТ-4У и факсимильного аппарата П-111.

Основным направлением информационного взаимодействия рассмотренных сетей и систем является поэтапное создание единой унифицированной автоматизированной стационарно-полевой сети документального обмена (ЕАСДО), предоставляющей услуги по обмену электронной корреспонденцией и телеграфной связи в интересах всех видов и родов войск ВС РФ.

На первом этапе необходимо обеспечить организацию составных многопротокольных трактов за счет межсетевого шлюзования и сопряжения протоколов на транспортном и сетевом уровнях. При этом развитие автоматизированной сети документальной связи возможно на базе КТС ОС с включением ЦКС в ЗС СПД, а также подключение оконечных средств обработки документальных сообщений к единой телекоммуникационной сети ВС РФ с общим адресным пространством.

На последующих этапах при разработке средств ЕАСДО следует использовать унифицированные протоколы документального обмена по каналам и трактам с применением средств шифрованной связи.

Сапунова Л.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МОДЕЛЬ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ С МЯГКИМ ДЕКОДИРОВАНИЕМ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ

Системы обмена данными (СОД) военного назначения выполняют функции передачи данных в автоматизированных системах управления (АСУ) с требуемой своевременностью, достоверностью и безопасностью обмена всеми видами информации. Эффективность функционирования СОД в АСУ определяется в основном вероятностно-временными характеристиками доставки сообщений и параметрами достоверности передачи данных на различных уровнях иерархии их функционирования.

Системы обмена данными строятся с использованием каналов связи различной физической природы, в том числе каналов КВ радио-, радиорелейной, тропосферной и спутниковой связи. Поэтому разработка систем повышения достоверности (СПД) для систем передачи данных военного назначения должна осуществляться с учетом воздействия на линии связи как случайных, так и преднамеренных помех. В условиях высокой нагрузки на сети передачи данных вероятностно-временные характеристики процессов обмена сообщениями в СОД в значительной степени зависят от обеспечиваемой системой скорости передачи данных. Поэтому, как правило, решаемые на практике задачи проектирования СПД направляются на обеспечение максимальной скорости передачи данных при обеспечении требуемой достоверности.

К настоящему времени достаточно хорошо изучены принципы построения СПД, функционирующих в условиях случайных помех с различной статистической структурой. Исследованы теоретические основы анализа и синтеза системы передачи данных, функционирующих в конфликтных условиях. Получены границы гарантированной помехоустойчивости передачи информации при заданной скорости передачи. Однако, вопросы применения эффективных

алгоритмов повышения достоверности на различных уровнях функционирования СПД, в условиях воздействия оптимизированных помех практически не изучены.

В настоящей работе рассматривается модель СПД, обеспечивающая возможность постановки и решения задач анализа и синтеза системы передачи данных на канальном уровне ЭМВОС, функционирующей в условиях оптимизированных помех. В отличие от других работ в предложенной модели учитывается возможность использования мягкого декодирования данных, поступающих с физического уровня системы и дополнительного повышения за счет этого эффективности функционирования СПД.

Сафронов Ю.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ СО СПЕКТРАЛЬНЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ПРОИЗВОДСТВА

Сегодня среди ведущих компаний телекоммуникационной техники идет серьезная конкуренция за рынок сбыта. Самые крупные компании задают общий темп рынку и занимают большие его сегменты, более мелкие компании занимают определенные ниши и становятся лидерами только в них. При этом между ними нет единых стандартов и зафиксированных предложений по вопросам каналообразования на канальном уровне. Это, во-первых, усложняет коммутацию оптических каналов внутри сегмента одного бренда и требует применения ROADM. Во-вторых, делает практически невозможным коммутацию каналов на оборудовании различных брендов.

Эта разница в стандартах является существенным препятствием для создания единого международного телекоммуникационного пространства с коммутацией оптических каналов.

Коммутация разноволновых каналов осуществляется с помощью перестраиваемых оптических мультиплексоров ввода-вывода (ROADM).

Применение различных по конструкциям ROADM имеет ряд ограничений, обусловленных, прежде всего, возможностями по доступу к оптическим каналам средствами оптических коммутаторов на основе различных технологий, величинами потерь мощности в оптических соединениях коммутаторов, уменьшением полосы пропускания оптического канала при каскадировании ROADM с пространственными оптическими фильтрами технологии AWG (Arrayed Waveguide Grating), требуемым временем реконфигурации и перестройки источников излучения в транспондерах.

При выходе из строя ROADM остается ограниченный объем коммутации, и основная часть действующих каналов по направлению связи теряется.

Так как сегодня на сетях связи функционирует большая номенклатура не стандартизированного оборудования волоконно-оптического оборудования связи то возникает проблема обучения обслуживающего его персонала и связанна с необходимостью обучения эксплуатации на каждом типовом образце средств связи. Подготовка таких специалистов долгое и дорогое удовольствие требующие от компании не только одноразового обучения персонала, но и прохождения ими дополнительных курсов.

Наглядным примером такого не стандартизованного оборудования являются модули SFP. Их задача - преобразование цифровых сигналов активных устройств сети в оптические, что вносит дополнительные задержки в работе линии связи. На данный момент единого стандарта разъема для приемо-передатчиков принято не было. В результате количество вариантов разъёмов для него у разных производителей давно перешло за сотню. Кроме интерфейса коммутатора и приемо-передатчика, требуется совместимость их протоколов обмена информации.

Делая общий анализ по ВОСП - СР, можно выделить два направления развития:

Первое внедрение в сетях различного назначения технологий, направленных на повышение эффективности ВОСП на основе методов волнового мультиплексирования в линейном спектре, т. е. потребуется создания стандарта для взаимодействия CWDM, DWDM и HDWDM оборудования различных производителей.

Второе направление развития ВОСП это разработка и внедрение стандартов типового каналообрзования для работы с системами спектрального уплотнения.

Саяркин Л.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ. АВТОМАТИЗИРОВАННЫЕ РАБОЧИЕ МЕСТА УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ, АНАЛИЗ ИХ УЯЗВИМОСТЕЙ И ОЦЕНКА НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В современном мире, мире инфотелекоммуникацинных технологий, проблемы, связанные с утечкой информации, являются наиболее актуальными. Не зря говорят: «Кто владеет информацией, тот владеет миром».

Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

В настоящее время обработка конфиденциальной и секретной информации есть неотъемлемая часть каждой успешной организации, в том числе и ВС РФ. Технологии продвинулись до того, что вредоносные закладки могут быть вписаны во flash-память BIOS и аппаратные средства компьютера. Для того, чтобы кибератака была предотвращена, и нужная информация не смогла бы «утечь», необходимо иметь достаточно надежные и защищенные аппаратные и программные средства. Существует аппаратно-программный модуль доверенной загрузки (далее АПМДЗ), предназначенный для защиты автономных и сетевых компьютеров от несанкционированного доступа.

Постоянное совершенствование технологий в области кибератак дает возможность через несовершенство средств доверенной загрузки получить доступ как к компьютеру «жертвы», так и соответственно к данным, составляющих сведения государственной тайны (что касается области Министерства обороны).

Чтобы избежать подобных случаев необходимо как минимум, постоянно искать несовершенства – уязвимости средств, тем самым, блокируя НСД в компьютер.

Модуль доверенной загрузки представляет собой комплекс аппаратно-программных средств (плата, аппаратные средства идентификации и аутентификации, программное обеспечение для поддерживаемых операционных систем), устанавливаемый на рабочее место вычислительной системы (персональный компьютер, сервер, ноутбук, специализированный компьютер и др.).

Важным элементом защиты от реализации программных угроз — обеспечение замкнутой программной среды.

Основная задача модулей доверенной загрузки – создание полноценной доверенной среды на автоматизированном рабочем месте. Под доверенной средой принято понимать состояние информационной системы, в которой используются аппаратные и программные средства способные обеспечить обработку информации разной категории секретности без нарушения прав доступа. И здесь нам приходится говорить о надежности программного обеспечения.

Оценка надежности программы будет осуществляться на основе известных заранее отказах программы или какого-то конкретного участка, что позволит рассмотреть общую картину надежности программы и сделать вывод – надежно или ненадежно данное программное обеспечение. Все расчеты будут производиться на основе известных статистических моделях оценки надёжности, таких как Миллса, Нельсона, Липова и простой интуитивной модели.

Математический аппарат данных алгоритмов позволяет с большой степенью точности определить вероятность надежной работы программы.

Сидорова А.П., Боровкова М.А., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ОТКРЫТОГО СЕГМЕНТА ОАЦСС НА ОСНОВЕ SIEM-ТЕХНОЛОГИИ

В настоящее время продолжается развитие и совершенствование Объединенной автоматизированной цифровой системы связи (ОАЦСС), на базе которой развертываются и функционируют современные мультисервисные сети, предоставляющие пользователям широкий набор услуг связи высокого качества. При этом одной из ключевых задач остается обеспечение высокой безопасности функционирования таких сетей, что особенно актуально в условиях их сопряжения с открытыми сетями операторов связи ЕСЭ РФ.

Оборудование УС ОАЦСС позволяет развертывать современные цифровые узлы связи, а на их основе создавать телекоммуникационные сети, в которых в зависимости от принадлежности той или иной госструктуре обрабатывается информация с различными уровнями конфиденциальности. При этом в открытом сегменте таких сетей, в связи с отсутствием жестких требований по обеспечению безопасности информации, мероприятия защиты сводятся, как правило, к установлению антивирусных средств и межсетевых экранов. Как показывает мировая практика, такие практически незащищенные сети становятся либо инструментом злоумышленников для доступа к закрытым сетям, либо источниками угроз со стороны инсайдеров.

В данной ситуации основным решением проблемы являются такие методы как анализ поступающей в сеть извне информации, ее фильтрация, проверка на достоверность и вредоносность, мониторинг сети и выявление подозрительной активности, как пользователей, так и приложений.

Наиболее эффективным методом решения данной задачи в открытом сегменте сети является применение SIEM (Security Information and Event Management) технологии, позволяющей уменьшить степень угрозы. SIEM объединяет технологию управления информационной безопасностью (Security Information Management) и технологию управления событиями безопасности (Security Event Management). SIEM обеспечивает анализ информации, поступающей с сетевых устройств и устройств

безопасности, приложений, их журналирование и создание отчетов и выявление сведений о внешних и внутренних угрозах практически в режиме реального времени.

SIEM не предотвращает вредоносные инциденты, но может обнаружить сетевые атаки, вирусные заражения, попытки несанкционированного доступа, ошибки и сбои в работе информационной системы, даже в том, когда все имеющиеся в системе средства защиты «молчат», так как отдельные инциденты могут не восприниматься ими как угроза или атака, что помогает их предотвратить в процессе дальнейшего функционирования системы.

Источниками информации для SIEM систем может служить практически любая информация от элементов инфотелекоммуникационной сети: антивирусных приложений, журналов событий серверов и рабочих станций, межсетевых экранов, систем веб-фильтрации, сетевого активного оборудования. Все эти источники присутствуют в открытом сегменте и при успешном внедрении SIEM систем можно добиться почти полной автоматизации процесса выявления угроз. Таким образом, SIEM технология является одним из наиболее перспективных направлений обеспечения безопасности функционирования открытого сегмента инфотелекоммуникационной сети, тем более, что последние SIEM-решения, имеющиеся на рынке, сочетают в себе функционал не только анализа данных, но и функции анализа трафика (анализ пакетов) и управления рисками.

Сныткин И.И., Кулюпин Е.Н.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ПЕРСПЕКТИВНЫХ СИСТЕМ ДВУКРАТНЫХ ПРОИЗВОДНЫХ КОДОВЫХ ДИСКРЕТНО-ЧАСТОТНЫХ СИГНАЛОВ С ЗАДАННЫМИ СВОЙСТВАМИ И АППАРАТНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЕЕ РЕАЛИЗАЦИИ

Реализуемые в настоящее время в радиотехнических телекоммуникационных системах (в частности, в системах передачи данных) алгоритмы (способы, математические модели) формирования дискретно-частотных сигналов (ДЧС) не позволяют обеспечить выполнение предъявляемых современных требований по помехоустойчивости, имитостойкости, энергетической и структурной скрытности, от которых напрямую зависит достоверность передаваемых сообщении в условиях радиоэлектронной борьбы (РЭБ) и информационного противоборства (ИПб).

В целях выполнения вышеуказанных требований предлагаются новые принципы (в том числе математическая модель) формирования ДЧС - на основе ансамблей двукратных производных управляющих числовых кодовых последовательностях фиксированной длины, которые, в свою очередь, формируются на основе поэлементного циклического сложения между собой значений элементов двух различных полей Галуа. Формируемые таким (предлагаемым) образом системы ДЧС именуются как системы двукратных производных кодовых дискретно-частотных сигналов (ДК ПКДЧС)).

В том числе, в докладе рассматривается техническое решение формирования систем ДК ПКДЧС с заданными свойствами. Особенностью предлагаемого решения является композиционное сочетание определенным образом в одном программно-управляемом устройстве двух блоков формирования элементов различных полей Галуа, многоразрядного параллельного сумматора по модулю с последовательным переносом и системного блока управления.

Предлагаемые математическая модель синтеза ДК ПКДЧС и реализующее ее техническое решение позволят практически обеспечить наибольшую степень неопределенности вида, формы, длительности, ансамблевых и других характеристик систем сигналов сложной формы по сравнению с известными формами и видами ДЧС, что особенно важно при применении этих сигналов в СПД в условиях активных РЭБ и ИПб.

Сныткин И.И., Балюк А.А.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М.Штеменко

МЕТОД АНАЛИЗА И РАСКРЫТИЯ "ТОНКОЙ" ВНУТРЕННЕЙ СТРУКТУРЫ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В настоящее время псевдослучайные последовательности (ПСП) любой структуры находят широкое применение в информационно-телекоммуникационных системах (ИТС) самого различного назначения. Выбор для использования конкретного вида ПСП осуществляется на основе оценки их системных параметров, таких как: помехоустойчивость, скрытность, имитостойкость и др. В целях решения задач обеспечения указанных системных параметров используются ПСП, основу практического применения которых составляют М-последовательности. Однако структура М-последовательностей подвержена эффективному раскрытию посредством широко известного алгоритма Берлекэмпа-Месси.

Альтернативу М-последовательностям составляют нелинейные рекуррентные последовательности (НЛРП). На сегодняшний день сформулированы правила построения НЛРП и

производных от них, существуют различные программные и технические решения их генерирования. Но до настоящего времени не изучены структурные свойства НЛРП и не существует алгоритма раскрытия их структуры и имитации. Данные обстоятельства являются препятствиями широкого применения НЛРП в различных ИТС.

В докладе предложен метод анализа и раскрытия "тонкой" внутренней структуры НЛРП на примере кодов квадратичных вычетов различных длительностей. На основе теории полей Галуа приводится математическое описание свойств и закономерностей внутренней структуры кодов. Благодаря выявленным закономерностям установлены и математически описаны зависимости между элементами НЛРП, разработан алгоритм раскрытия их структуры. Рассматриваются основные категории и принципы этого алгоритма. Рассматривается разработана программа для ЭВМ раскрытия структуры НЛРП в виде кодов квадратичных вычетов, позволяющая по установленному значению максимальной длины последовательности (Lmax=p, GF(p), p - простое число) определять, какое количество ее символов необходимо для раскрытия структуры всего кода, а также при известности данных символов восстанавливать всю последовательность.

Сныткин И.И., Енин Н.Н.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М.Штеменко

НОВЫЕ ПРИНЦИПЫ И МЕТОД ЭФФЕКТИВНОЙ АДРЕСАЦИИ СТРУКТУРНЫХ ЭЛЕМЕНТОВ ПАКЕТНЫХ СЕТЕЙ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ПРИМЕНЕНИЯ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ НЕЛИНЕЙНОЙ СТРУКТУРЫ

На основе анализа существующих и перспективных протоколов адресации элементов телекоммуникационных сетей СПД IPv4, IPv6, TCP и др. показывается, что установленные требования «ГОСТ Р.ИСО 7498-99. Базовая модель защиты информации» по услугам и механизмам защиты информации на 3-м (сетевом) уровне модели OSI/ISO не могут быть реализованы в рамках протоколов IPv4 и др. Показывается, что тетрадная 8-битовая структура адресного поля данных протоколов, а также известные динамические протоколы адресации принципиально не позволяют выполнять эти требования ГОСТа, тем более в условиях активных РЭБ и информационного противоборства (ИПб).

В этой связи предлагается обеспечивать эти требования ГОСТа посредством применения в качестве адресных идентификаторов кодовые формы, реализующие принцип неполного динамического кодирования с изменяющейся длительностью адресного поля с шагом до 1 бита на основе сигнально-кодовых конструкций нелинейной структуры (СКС НС) небольшой длины la с Δla≈1 бит, обработка которых на приемной стороне может осуществляться помимо дешифраторных и корреляционными методами.

Реализация такого пути возможна на основе использования нелинейных рекуррентных последовательностей (НЛРП) в виде кодов квадратичных вычетов (ККВ), характеристических кодов (ХК) и других кодов (Холла, Якоби. Зингера), существующих в полях Галуа GF(p), GF(pn), где p - простое число, n = 1,2,3,4,.. , для длительностей {ℓ}={p, p-1, pn-1}= {4t+1, 4t+3, 4t, 4t+2}, t=1,2,3...[43]. Такие НЛРП обладает абсолютной линейной сложностью (АЛС) (т.е. скрытностью) АЛС=ℓ, или относительной линейной сложностью ОЛС=ℓ/ℓ=1 (100%). Это означает, что для раскрытия НЛРП необходимо знать, по существу, всю структуру НЛРП длительностью ℓ. Поэтому применение НЛРП для процедур адресации делает их незаменимыми с точки зрения обеспечения высокой скрытности.

В докладе рассматриваются потенциальные возможности НЛРП для использования в процедурах адресации, принцип и методический аппарат 3-х новых способов адресации, основанных на использовании НЛРП: 1 способ – «фиксированных тетрад» (ФТ), 2-й способ – «динамических тетрад» (ДТ), 3 способ – «динамического блочного трансляционного двоичного кодирования» (ДБТДК), оцениваются системные и скрытностные свойства этих способов. Применение указанных способов позволит достичь высоких показателей скрытности и имитостойкости процесса адресации.

Соловьев В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ ПРОБЛЕМЫ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Чтобы разбираться в современных угрозах безопасности информации, требуется огромный спектр знаний - от языков программирования Go и JS до диалектов арабского языка, от особенностей прошивок жестких дисков до теории шифрования данных. Более того, не существует модели угроз безопасности информации универсальной и действенной для всех. Каждый объект информатизации имеет уникальный набор элементов ИТ-инфраструктуры, со своими уязвимыми местами и потенциальными точками проникновения. Естественно, нет единого, рецепта защиты.

Используемые в настоящее время методики моделирования угроз и оценки защищенности информации от несанкционированного доступа на объектах информатизации различного назначения основаны и регламентируется следующими руководящими документами:

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 25.07.2011) "О персональных данных";
2. Методические документы ФСТЭК РФ:

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах» (2015 года);

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (15 февраля 2008 года);

– приказ ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. N 17;

– меры защиты информации в государственных информационных системах (Утвержден ФСТЭК России 11 февраля 2014 г.).

– моделирование можно рассматривать как замещение исследуемого объекта (оригинала) его условным образом, описанием или другим объектом, именуемым моделью и обеспечивающим близкое к оригиналу поведение в рамках некоторых допущений и приемлемых погрешностей.

Действительная польза от моделирования угроз безопасности может быть получена только при соблюдении двух условий:

– модель угроз обеспечивает корректное (адекватное) отображение свойств оригинала, существенных с точки зрения исследуемой операции;

– модель угроз позволяет устранить проблемы, присущие проведению исследований на реальных объектах.

Конечная цель моделирования угроз БИ в информационных системах различного назначения – выявлять недостатки, разработке мер по их устранению.

У используемых в настоящее время моделей в системе защиты информации есть ряд недостатков, не позволяющих напрямую использовать их для моделирования угроз и оценки защищенности, а именно:

– производится качественная (вербальная) оценка угроз безопасности информации;

– реализуется детерминистский подход, не учитывающий стохастическую природу неопределенности процесса реализации угроз и динамику процесса защиты информации в целом;

– структура объекта информатизации и угрозы оцениваются экспертным методом, качество результатов применения которого определяется уровнем подготовки экспертов;

– не в полной мере учитывается человеческий фактор;

– не полностью учитывается вариативность сценариев реализации НСД и динамические характеристики процесса защиты информации.

В условиях массированных кибер-атак, характерных для информационного противоборства, такой подход может привести к принятию необоснованных решений по защите информации от несанкционированного доступа.

Угроз и типов атак стало так много, что проанализировать их «вручную» и построить качественную модель угроз также становится сложнее. Аналогом книги «Компьютерные вирусы изнутри и снаружи» о вирусах Криса Касперски 2006 года сейчас являются петабайты данных, неалгоритмизируемый опыт и навыки экспертов. Необходимо строить системы машинного обучения, которые возьмут на себя рутинные операции по сбору информации об уязвимостях и системах информатизации. Так, требуется создать централизованную автоматизированную систему, способную собирать и обрабатывать данные по всем уязвимостям и строить модели угроз для каждой информационной системы, в первую очередь – для объектов критической инфраструктуры.

Это направление развивают в США: начиная с июня 2016 года, объединенная команда ученых из восьми университетов мира планирует обучить искусственную интеллектуальную программу IBM Watson по специальности «информационная безопасность».

Старков А.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРОБЛЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

Виртуальные вычислительные сети (VLAN) - логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной

физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

В процессе жизнедеятельности сети происходит ее реструктуризация: количество подразделений и военнослужащих, их территориальное расположение меняется. Возникает проблема оперативного переопределения приоритетов, разграничения доступа единичным пользователям и группам пользователей, при этом обеспечивая минимальные затраты на устанавливаемое оборудование. Решение в сложившейся ситуации является использование VLAN. Применение данной технологии позволит:

- уменьшить количество широковещательного трафика в сети, тем самым увеличится производительность сети без замены или добавления дополнительного оборудования;
- создать группы пользователей по их функциональному, а не территориальному назначению, а также вносить в них изменения без изменения физической инфраструктуры и отсоединения пользователей и серверов от сети,
- повысить безопасность сети за счет невозможности пользователей одной группы попасть к пользователям другой группы.

Во многих фирмах и провайдерах интернета давно используется данная технология.

VLAN обеспечивает гибкость в разработке и внедрении инфраструктуры коммутируемой сети. Сети VLAN является частью любой серьезной сетевой разработки, но системному администратору необходимо понимать потребности пользователей и пути потоков информации до внедрения виртуальных сетей. Данная технология при всей своей полезности имеет и ряд недостатков, с которыми приходится считаться. Раньше наиболее частой была проблема совместимости оборудования: не все коммутаторы и хабы умели безболезненно пропускать тегированные кадры, и не все сетевые адаптеры поддерживали увеличенный размер кадра. Сейчас вероятность столкнуться с таким сетевым устройством очень мала. Поэтому на первый план выходит необходимость вручную настраивать каждый порт каждого коммутатора. При часто меняющейся топологии сети возникает ситуация, когда необходимо за кратчайший промежуток времени внести изменения в топологию сети, при этом сохраняя высокий показатель производительности и безопасности. Зачастую большое количество настроек коммутационного оборудования и отсутствие полной карты логических соединений не позволяет это сделать. В данном месте возникает проблема оптимизации работы системного администратора по определенным алгоритмам, которые должны анализировать предложенную топологию сети и выдавать наиболее оптимальную схему построения VLAN, а также какие внести изменения в сложившейся ситуации, чтобы обеспечить подключение новых клиентов и серверов.

Троянов Я.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ХЭШ-ФУНКЦИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МЕХАНИЗМОМ

В ходе автоматизации технологического процесса, так или иначе, приходитс я сталкиваться с использованием телемеханики. Телемеханика – это совокупность методов и технических средств, предназначенных для передачи и приема информации с целью дистанционного управления оборудованием и контроля его работы. Одним из каналов передачи информации может служить радиоканал. Телемеханику, в которой для передачи команд управления и контроля используют каналы радиосвязи, называют радиотелемеханикой. При работе по радиоканалу, всегда стараются добиться: обеспечения высокой достоверности передаваемой информации; сокращения времени запаздывания сигналов; высокой надёжности передачи команд управления; высокой степени автоматизации процессов сбора информации. Но гораздо реже ставят цель обеспечения безопасности передачи информации.

На первый взгляд это может показаться не столь важным пунктом, в перечне основных целей, но если задуматься о возможности умышленного искажения информации и подачи ложных команд, то станет ясно насколько данная проблема актуальна. Сейчас большинство предприятий автоматизировано и многие из них управляют своим технологическим процессом посредством радиотелемеханики, слабая защищенность которой, может привести к неправильной работе предприятия или даже к аварии. Таким образом, защита от случайного или преднамеренного воздействия на систему телемеханики, становится очень важной частью разработки системы.

Одним из способов защиты, может служить использование распространенной технологии хэширования сообщений.

Хэш-функции широко применяются для обеспечения безопасности, например в электронной цифровой подписи, или аутентификации. Основная задача хэш-функций – генерация дайджестов, уникальных для конкретного документа, то есть в получении из сообщения произвольного размера,

значения фиксированного размера. При этом изменяя исходные данные хоть на один бит, мы получим совсем другое число на выходе.

Основные свойства хэш-функции:

1. На вход хэш-функции подается сообщение произвольной длины;
2. На выходе хэш-функции формируется блок данных фиксированной длины;
3. Значения на выходе хэш-функции распределены по равномерному закону;
4. При изменении одного бита на входе хэш-функции существенно изменяется выход.

Для обеспечения устойчивости хэш-функции к атакам она должна удовлетворять следующим требованиям:

1. Если мы знаем значение хэш-функции *h*, то задача нахождения сообщения M такого, что H(M) = *h*, должна быть вычислительно невозможной;

2. При заданном сообщении M задача нахождения другого сообщения M', такого, что H(M) = H(M'), должна быть вычислительно невозможной.

Хэш-функции строятся на многократном повторении математических действий, когда исходное сообщение раскладывается на отдельные блоки фиксированного размера, и над этими блоками выполняются преобразования. Часто в ходе преобразования, блоки сжимаются, так как выход обычно меньше по размеру, чем блок, подаваемый на вход.

Труфанов С.К., Шерстюк М.Ю., Мач Д.П.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

ТИПОВЫЕ МЕТОДЫ ОБРАБОТКИ ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА ИНФОТЕЛЕКОММУНИКАЦИЙ

В современных инфотелекоммуникационных системах событийный мониторинг может применяться для решения задач анализа и контроля происходящих в них процессов. Под первичными данными событийного мониторинга инфотелекоммуникационных систем понимается совокупность событий, характеризующих последовательность происходивших в инфотелекоммуникационной системе фактов. Это могут быть, к примеру, события об изменении состояний сетевых элементов в сети, а также собственные события управления конфигурацией системы мониторинга.

Количество фиксируемых в инфотелекоммуникационной системе событий в единицу времени, как правило, настолько велико, что для выполнения ручного анализа данных событийного мониторинга представленных, например, в виде журнала событий, требуется целый отдел экспертов-аналитиков, что влечет за собой значительные трудовые затраты, и кроме того, увеличивает вероятность ошибки обработки данных или вовсе их игнорирование по причине усиления роли человеческого фактора. Альтернативный метод обработки данных событийного мониторинга — применение автоматизированной обработки данных с использованием таких типовых методов обработки фактографических данных, как:

- фильтрация событий по правилу отбора;
- агрегация событий по задаваемому обобщающему правилу;
- методы статистической обработки по расчету количественных мер;
- интеллектуальный анализ данных по поиску возникающих инцидентных ситуациях на основе алгоритмически заданных правил поиска зависимостей между событиями;
- -нализ данных посредством построения сводных таблиц с выбранными измерениями и мерами;
- построение обобщающих графиков самого разного вида для упрощения вторичного анализа данных аналитиком-экспертом.

Под фильтрацией понимается отсеивание событий, не несущих значительной смысловой нагрузки для решения актуальной в данный момент задачи. Фильтрация может осуществляться как на этапе сбора первичных данных событийного мониторинга, так и на этапе отображения журнала событий в графических приложениях.

Применение агрегации позволяет преобразовывать совокупности событий в новые события, сокращая объем данных событийного мониторинга и повышая их наглядность для анализа должностными лицами. Эти события являются вторичными данными мониторинга.

Статистическая обработка данных заключается в вычислении основных статистических показателей, таких как, к примеру, математическое ожидание, среднеквадратичное отклонение и дисперсия, которые могут помочь при принятии решения должностным лицом. Для нечисловых атрибутов событий может быть рассчитана частота появления того или иного строкового значения.

Интеллектуальный анализ данных, как правило, заключается в переборе всех накопленных данных событийного мониторинга, либо только что собранных, и применение к ним набора правил. Правила выполняют поиск зависимостей между событиями по алгоритму поиска, который разрабатывается экспертом-аналитиком. Однако, сам алгоритм поиска может быть составлен с использованием совершенно различных областей знаний, например, с использованием нейронных сетей.

Анализ с применением OLAP-технологии обработки данных требует категоризации данных для поиска общих измерений данных и количественных мер их оценки. В качестве меры может быть использовано количество событий, либо математическая функция от какого-либо общего для всех событий числового атрибута. Эксперту-аналитику в таком случае предоставляется инструмент для анализа данных в виде двумерной таблицы с возможностью группировать события в любом порядке следования измерений по двум осям и вычисления мер в соответствии с выбранной группировкой событий. Простейший пример — посчитать количество событий с разбиением на годы, месяца и дни, либо по дням недели и часовым интервалам. Для оценки эффективности реализации анализа данных его механизм должен быть проверен на предмет удовлетворения требованиям теста FASMI.

Под обобщенными графиками понимаются точечные линейные графики, гистограммы и диаграммы различных форм.

Тюмин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОЦЕНКА СВОЕВРЕМЕННОСТИ ПЕРЕДАЧИ СИГНАЛОВ БОЕВОГО УПРАВЛЕНИЯ И ОПОВЕЩЕНИЯ

Для повышения надежности, а, следовательно, и вероятности своевременного доведения сигналов используют тракты передачи сигналов боевого управления и оповещения. Серьезные затруднения, связанные с осуществлением групповой синхронизации последовательностей, передаваемых по отдельным каналам связи, обуславливают необходимость раздельного приема и выделения сигналов в каждом приемнике сигналов боевого управления и оповещения, количество которых равно количеству используемых в тракте каналов связи. Поэтому в составе тракта целесообразно использовать групповое устройство, предназначенное для приема, обработки и выдачи сигналов боевого управления и оповещения на устройство отображения, а также для выдачи сигналов в передатчик сигналов подтверждения. Введение группового устройства в состав тракта передачи сигналов боевого управления и оповещения, позволяет осуществлять дополнительную обработку сигналов, поступающих в него из преемников сигналов боевого управления и оповещения. Суть этой обработки заключается в том, что в групповом устройстве происходит сравнение сигналов, принятых из приемников, и на устройство отображения выдается сигнал, прошедший проверку по «большинству», причем, если сигнал получен только с одного приемника, он выдается на устройство отображения, если сигналы получены с двух приемников, то они сравниваются между собой и в случае их совпадения сигнал выдается на устройство отображения, в противном случае они стираются, если сигналы получены с трех приемников - осуществляется их обработка «по большинству», причем эти сигналы стираются только в том случае, если все они отличны друг от друга и т.д. В случае стирания сигналов в групповом устройстве в передатчик сигналов подтверждения ничего не выдается.

Рассмотренный алгоритм обработки сигналов боевого управления и оповещения в групповом устройстве позволяет несколько повысить достоверность доведения сигналов от отправителя до получателя, по сравнению с алгоритмом выдачи сигнала на устройство отображения сигналов боевого управления и оповещения через схему «или», которым пользуются, например, в табельной аппаратуре передачи сигналов оповещения военного округа.

Таким образом, групповое устройство является своего рода решающей схемой, в которой принимается окончательное решение на выдачу сигнала боевого управления или оповещения на устройство отображения или его стирание.

Фёдоров П.Н., Сазонов В.В., Зубакин В.В., Ванчугов А.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

О НЕОБХОДИМОСТИ РАЗРАБОТКИ ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ОБМЕНА ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящее время существующие методы оценки качества передачи информации в сетях обмена электронной корреспонденцией (СОЭК) специального назначения имеют следующие недостатки:

- проведение измерений, а также анализ их результатов занимают продолжительное время;
- необходимо привлекать опытных специалистов (администраторов и операторов);
- невозможность в большинстве случаев проведения экспериментов без нарушения режима эксплуатации СОЭК.

Одним из наиболее эффективных методов исследования, снижающих вышеуказанные недостатки, является имитационное моделирование, сущность которого заключается в имитации процессов функционирования исследуемой системы с целью получения её характеристик. К группе

средств, моделирующих работу СОЭК, можно отнести ComNet от CACI Products Company, OPNET от OPNET Technologies, OMNeT++, NS-3, AnyLogic, Cisco Packet Tracer, NetCracker.

Каждая из этих систем предназначена для решения конкретных задач разной степени абстракции. Анализ средств имитационного моделирования показывает, что одним из наиболее эффективных продуктов, предназначенных для моделирования компьютерных сетей всех типов, а также имитации процессов в созданных сетях, является пакет Net Cracker Professional фирмы Net Cracker Technology. С его помощью могут быть решены такие задачи, как определение производительности сети при заданной топологии и рабочей нагрузки.

Рассматривая вопросы построения имитационной модели работы СОЭК специального назначения, необходимо:

– на первом этапе составить обобщенную структуру системы, которая включает в себя сбор информации о расположении рабочих станций, серверного и сетевого оборудования, о стандартах и спецификации всех физических соединений между вышеперечисленными устройствами;

– на втором этапе необходимо осуществить анализ функционирования составных элементов данной системы и сделать выводы о степени адекватности разрабатываемой модели.

Планируемым результатом данных исследований является разработка имитационной модели СОЭК специального назначения, позволяющая оценить эффективность её функционирования при различных технологиях построения транспортной сети, без нарушения режимов эксплуатации реально действующих СОЭК специального назначения.

Федотов Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПОДХОД К ВЫЯВЛЕНИЮ АНОМАЛИЙ В МАССИВЕ ДАННЫХ ОТ РАЗНЫХ ИСТОЧНИКОВ ДАННЫХ

В настоящее время существует комплекс проблем, возникающий при работе с большими объемами данных. Одной из таких проблем является обнаружение отклонений от нормальных значений набора данных, свойственных как одному, так и группе объектов информационной среды (ИС), получаемых от разных источников.

В настоящем докладе предлагается подход к выявлению аномалий данных на основе построения групповых паттернов поведения в данных от разнородных источников.

Предполагается, что начальными условиями являются некоторые наборы данных, описывающих один атрибут состояния объекта, находящихся в ИС, но получаемых от различных источников. Логи разных источников данных имеют различный набор атрибутами, но в них обязательно присутствует идентификатор объекта, и метка времени, когда было зафиксировано состояние объекта, что позволяет синхронизировать их значения. В рассматриваемом в докладе примере один источник данных является статическим, т.е. его положение в пространстве остается неизменным, а второй источник данных является динамическим, и его положение в пространстве определяется некоторым маршрутом. Кроме того, данные от первого источника обладают меньшим уровнем детализации, в то время как второй источник дает больше информации об атрибуте объекта, но в силу динамичности его положения, полученные от него данные недостаточно полны. Таким образом, необходимо разработать подход, позволяющий выявить паттерны поведения объектов системы и аномалии в них путем анализа и корреляции данных от разных источников.

Существует несколько подходов к корреляции данных от разных источников данных – методами автоматической обработки или методами визуализации данных путем построения множества взаимосвязанных моделей графического представления данных. В докладе предлагается совмещение этих двух способов, поскольку в первом случае алгоритмы автоматической корреляции представляют собой некоторый черный ящик, требующего дополнительного объяснения конечным пользователям, а методики визуализации требуют предварительной обработки входных данных для снижений их размерности для получения легко воспринимаемого изображения.

Предлагаемый подход состоит из двух этапов. На первом этапе происходит нормировка значений атрибутов, получаемых от разных источников. В данном случае диапазон значений, получаемых от второго источника, отображается на множество значений атрибута, получаемого от первого источника с сохранением исходного уровня детализации. На втором этапе формируется множество моделей визуализации, предназначенных для отображения динамики и сравнения данных от разных источников. Выбор моделей визуализации зависит от природы значений атрибутов. В исследуемом примере атрибут описывает положение объекта в пространстве, поэтому данные от источников данных можно трактовать как траектории в пространстве и отображать с помощью карт или графов. В этом случае граф сравнений также будет иметь вид карты или графа, и отклонения от маршрута объекта будут четко видны.

Фисенко М.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОЦЕНКА ЖИВУЧЕСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Современные промышленные системы давно вышли за рамки простых релейных систем, слабо подверженных угрозам. Промышленная система сегодня – это сложнейший комплекс, состоящий из персональных и панельных компьютеров, PLC, активного и пассивного оборудования. Такая сложная система не может обходиться без автоматизированного управления (АСУ) на всех уровнях.

Крайне важно понимать, что такие системы весьма уязвимы. Они могут быть подвержены различного рода внешним или внутренним угрозам.

Понятие «живучести» в технической литературе используется и применяется при создании технических систем различного назначения. Интерес к этой характеристике, как в теоретическом, так и в практическом отношении велик.

Под угрозами АСУ понимается возможность появления таких событий или обстоятельств, при которых могут быть негативные воздействия на информацию, обрабатываемую в данной системе, и что может привести к неправильной работе или к остановке в т.ч. производственных процессов. В качестве основных негативных воздействий рассматривается нарушение конфиденциальности, целостности и доступности обрабатываемой в АСУ информации.

Все источники угроз можно классифицировать следующим образом:

- по отношению к АСУ: на внешние и внутренние;
- по происхождению: на естественные (стихийные и техногенные) и антропогенные.

Приведем некоторые примеры источников угроз в каждой группе:

1. Внешние антропогенные: посетители, обслуживающие организации, внешние злоумышленники и др.
2. Внутренние антропогенные: вспомогательный персонал, инженерно-технический персонал и т.п.
3. Внешние техногенные: энергетические сети, транспорт и т.п.
4. Внутренние техногенные: количественная и качественная недостаточность компонентов АСУ (аппаратные средства, программные средства, инженерно-технические средства и т.п.).
5. Стихийные: стихийные источники угроз (наводнение, ураган, землетрясения, климатические явления).

В связи с этим аппаратно-программные средства подобной системы должны соответствовать следующим основным требованиям:

- в режиме реального времени обеспечивать работу системы управления;
- быть способными функционировать в сложных условиях, где могут быть большие перепады температур, загрязненная атмосфера, сильные электромагнитные поля и помехи, вибрационные и ударные нагрузки и т.п.;
- иметь возможность встраивания аппаратуры в основное оборудование;
- обладать высокой надежностью (на уровне надежности основного оборудования).

Таким образом, под живучестью АСУ понимается ее способности восстанавливать свой функционал и поддерживать значения основных эксплуатационных показателей в допустимых диапазонах при непредусмотренных регламентом нормальной работы неблагоприятных воздействиях внешней среды посредством использования специальных механизмов адаптации, рационального перераспределения имеющихся ресурсов, введения избыточности и проведением организационно-технических мероприятий на этапе.

Для оценки живучести АСУ необходимо разработать модель ее функционирования в условиях воздействия дестабилизирующих факторов. При этом оценка способности системы сохранять и восстанавливать свою работоспособность должна осуществляться за счет целенаправленной перестройки своей структуры, изменения режима (алгоритма) и параметров функционирования и (или) перераспределения располагаемых ресурсов. Кроме того, живучесть АСУ может обеспечиваться и проведением ряда организационных и инженерно-технических мероприятий: резервирования, комплексного применения средств управления, организации резервных каналов управления, подготовки и проведения мероприятий по восстановлению нарушенного управления и др.

Харитоненко В.Г.
Россия, г. Краснодар, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЯ ПРИ ИДЕНТИФИКАЦИИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Несмотря на широкое внедрение сетевых технологий и возможности в настоящее время передачи информации в электронном виде, объем переписки и документооборота с каждым годом растет и влечет за собой необходимость автоматизированной проверки документов на наличие в них информации ограниченного распространения.

Операции по оценке степени конфиденциальности информации выполняются довольно часто, но средств, позволяющих автоматизировать эту операцию, на настоящий момент времени неизвестно. Существует так же достаточно большое количество примеров (как в мирное время, так и в период проведения контртеррористических операций), подтверждающих актуальность данного вопроса.

Задача по идентификации степени конфиденциальности информации пересекается с задачей распознавания смысла. В настоящее время задача по распознаванию (формализации) смысла является важной, нерешенной задачей.

Важность этого вопроса так же подчеркивается тем, что задача по созданию многоязычных семантических поисковых Интернет-систем включена в план фундаментальных исследований Российской академии наук до 2025 года. Из этого следует вывод о том, что при создании данной системы, речь может идти о создании системы поддержки принятия решения. Система идентифицирует в тексте документа необходимые данные и обозначает их. Окончательное решение об уровне конфиденциальности информации принимает человек.

Необходимым условием для работы такой системы является наличие базы знаний, которая является неотъемлемой частью любой экспертной системы.

Экспертная система – это программный комплекс, использующий знания экспертов и процедуры вывода для решения конкретной задачи. В базе знаний представлены знания экспертов в конкретной предметной области, т.е. экспертов по определению степени конфиденциальности информации. На основе многолетнего опыта разработки экспертных систем задачи, для которых эти экспертные системы разрабатывались и приносили значительные результаты, были классифицированы.

В соответствии с данной классификацией, задача по определению степени конфиденциальности информации относится к задачам интерпретации (интерпретация – процесс определения смысла данных, т.е. построения описаний по наблюдаемым данным). База знаний экспертной системы представляет собой модель предметной области, описанную на языке сверхвысокого уровня, другими словами – модель всех существующих конфиденциальных данных. Экспертные системы являются подклассом более общего понятия – понятия интеллектуальных систем.

Результатом работы интеллектуальной системы поддержки принятия решения при идентификации степени конфиденциальности информации является:

- выделение в анализируемом тексте словоформ, в своей совокупности формирующих конфиденциальную информацию;
- выдача номера пункта Перечня сведений, конфиденциального характера;
- выдача предварительного заключения о степени конфиденциальности информации.

Интеллектуальная система поддержки принятия решения при идентификации информации ограниченного распространения может применяться как на персональных ЭВМ, так в локальных и глобальных информационных сетях.

Хушкин Д.П., Ноздрачёв Л.И., Бударин Э.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ВОЙНЫ

В современном обществе коммерческая разведка и электронный шпионаж стали, к сожалению, распространенным явлением в отраслях наукоемких технологий.

И как результат, информация всё чаще рассматривается информационной войной как потенциальное оружие.

При определении понятия информационной войны можно сказать, что это любое действие по использованию, разрушению, искажению информации конкурента и её функций; защите нашей информации против подобных действий и использованию наших собственных информационных функций.

Исходя из данного определения можно утверждать следующее.

Информационная война — это любая атака против информационной функции, независимо от применяемых средств.

Современные технологии позволяют конкуренту (противнику) изменить или создать информацию без предварительного получения фактов и их интерпретации.

Поражающие свойства информационного оружия направлены в первую очередь на человека. Особенно опасно, если воздействие осуществляется на мозг человека (трансформируется матрица памяти – искусственная амнезия на определенный период). Подобные изменения могут осуществляться программными закладками: речь в речи (акростих); изображение в изображении.

Создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях, - это естественная защитная реакция на появление нового оружия. Экономическую и научно-

техническую политику подключения государства к мировым открытым сетям следует рассматривать, прежде решив вопрос национальной информационной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна предусматривать защиту сетевого оборудования на территории страны от проникновения в него скрытых элементов информационного оружия. Это особенно важно сегодня, когда осуществляются массовые закупки зарубежных информационных технологий. Очевидно, что без

Оперативный доступ к информационным и вычислительным ресурсам, поддерживаемым сетью Интернет, дает возможность преодоления международной экономической и культурной изоляции, преодоления внутренней дезинтеграции, развития социальной инфраструктуры. Однако следует учитывать, что участие России в международных системах телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности.

Особенно остро проблемы защиты собственных информационных ресурсов в открытых сетях встают перед странами, которые технологически отстают в области информационных и телекоммуникационных технологий от США или Западной Европы. Сегодняшнее состояние российской экономики, неразвитость информационной инфраструктуры, неподготовленность российских пользователей к эффективной работе в сетях открытого информационного обмена не позволяют реализовать полноценное участие страны в таких сетях и пользоваться всеми возможностями новых технологий.

Обозначим практические мероприятия программного характера по защите от информационного оружия.

1. Организация мониторинга и прогнозирования потребностей экономических и других структур в различных видах информационного обмена через международные сети. Возможно создание специализированной структуры для контроля трансграничного обмена, в том числе посредством Интернета; координация мер государственных и негосударственных ведомств по предотвращению угроз информационной безопасности в открытых сетях; организация международного сотрудничества.

2. Разработка государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных и корпоративных сетей к мировым открытым сетям при соблюдении требований безопасности информационных ресурсов.

3. Организация системы комплексной подготовки и повышения квалификации массовых пользователей и специалистов по информационной безопасности для работы в мировых информационных сетях.

4. Разработка национального законодательства в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей открытых мировых сетей. Установление перечня информации, не подлежащей передаче по открытым сетям, и обеспечение контроля за соблюдением установленного статуса информации. Активное участие в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей.

Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек-Балтика М»

ОСНОВНЫЕ ПРОФИЛИ БАЗОВОЙ ТЕХНИЧЕСКОЙ АРХИТЕКТУРЫ АСУ СВЯЗЬЮ

Сложность создания и развития современных АСУ связью обусловливает в том числе интерес к различным подходам к декомпозиции и формализации таких систем в разных аспектах их представления. Одним из таких подходов является применение формализма базовой технической архитектуры, которая определяет профили и основные компоненты в многоуровневой архитектуре подсистем технической основы современной АСУ связью.

Системотехнические решения по построению каждого из профилей АСУ связью и каждой ее подсистемы должны базироваться на следующих соотношениях основных понятий:

- профиль определяет построение одной или нескольких подсистем;
- подсистема функционально представляет собой одну или несколько служб (сервисов);
- каждый сервис (служба) предоставляет одну или несколько услуг.

Основными профилями базовой технической архитектуры АСУ связью являются:

- функциональный профиль;
- профиль программно-технической реализации;
- профиль информационной безопасности.

Функциональный профиль определяет построение следующих подсистем:

- подсистем, реализующих платформу базовых инфотелекоммуникационных технологий и сервисов
- подсистем, реализующих комплексы прикладных информационно-аналитических сервисов организационного и оперативно-технического (технологического) управления.

К платформе базовых (инвариантных) инфотелекоммуникационных технологий и сервисов можно отнести подсистемы телекоммуникационных, офисных, геоинформационных, информационно-справочных сервисов, а также сервисов документальной поддержки управления, комплексного учета и комплексного мониторинга функционирования компонентов АСУ связью и ее объектов мониторинга и управления.

Функциональный профиль в части подсистем, реализующих комплексы прикладных информационно-аналитических сервисов организационного и оперативно-технического (технологического) управления определяет модель прикладных сервисов управления связью как услуг взаимосвязанных типовых функциональных процессов: учет, планирование, мониторинг, оперативный контроль, управление (как управляющие воздействия различного характера), ретроспективный анализ.

Профиль программно-технической реализации определяет открытую унифицированную архитектуру распределенной инструментально-технологической основы АСУ связью, к которой могут быть отнесены распределенные вычислительные сети и функционирующая в их среде базовая унифицированная инструментально-технологическая основа:

- подсистема построения функционального программного обеспечения;
- подсистема повышения надежности хранения данных и устойчивости функционирования программного обеспечения.

Основными компонентами подсистемы построения функционального программного обеспечения являются:

- подсистема разграничения доступа на прикладном уровне (рамочного характера);
- программная среда реализации выполнения, взаимодействия, синхронизации и коммуникации локальных и распределенных прикладных вычислительных процессов;
- подсистема ведения распределенной разнородной фрагментированной информационной базы.

Профиль информационной безопасности определяет построение подсистемы защиты информации в рамках технической основы АСУ связью и охватывает все уровни ее архитектуры.

Совокупность базовой функциональной архитектуры и базовой технической архитектуры образует концептуальный облик АСУ связью, давая возможность сопоставить ее функциональные возможности и ее техническую реализацию как две основных стороны рассмотрения (представления).

Шерстюк К.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

СПОСОБЫ ЦЕНТРАЛИЗОВАННОГО ОБНОВЛЕНИЯ УСЛОВНО-ПОСТОЯННЫХ ДАННЫХ В ИЕРАРХИЧЕСКИ ОРГАНИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В ряде случаев в иерархически организованных автоматизированных системах возникают задачи, связанные с централизованным обновлением условно постоянных данных. В качестве данных, требующих периодической актуализации, могут выступать, например, базы данных антивирусных средств, различные документы, конфигурационные файлы и т.д.

Если отдельные узлы данной автоматизированной системы функционируют под управлением операционных систем семейства Linux, то в этом случае данные возможно актуализировать посредством использования протоколов SSH или RSYNC.

В рамках решения данной задачи было разработано программное средство, позволяющее производить централизованное обновление с использованием любого из вышеназванных протоколов.

Для обновления данных через SSH был разработан программный компонент, позволяющий целиком автоматизировать выполнение консольных команд путем эмуляции действий пользователя, от лица которого происходит выполнение процедуры актуализации данных.

Данное программное средство позволяет производить обновление данных, используя в качестве их источника любой старший или одноранговый узел иерархии, что в свою очередь позволяет распределять сетевые нагрузки на отдельные узлы системы.

Обновление посредством протокола RSYNC имеет ряд преимуществ по сравнению с SSH, т.к. не требует установки дополнительного программного обеспечения, а также обеспечивает возможность шифрования, сжатия, сохранения прав доступа передаваемых данных и многое другое. Для обеспечения автоматизации процесса обновления достаточно добавить соответствующую команду в планировщик задач.

Механизм обновления данных с использованием любого из этих протоколов может быть организован с использованием авторизации по ключевой паре (открытый и закрытый ключ), что в свою очередь не требует хранения паролей доступа к источникам данных в открытом виде, а значит, снижает угрозу безопасности коммуникаций.

Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек-Балтика М»

СОБЫТИЙНО-ОРИЕНТИРОВАННОЕ ПОСТРОЕНИЕ ПРОЦЕССОВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ИНФОТЕЛЕКОММУНИКАЦИЯМИ

Автоматизация управления иерархически организованными, гетерогенными и динамичными инфотелекоммуникационными сетями представляет собой сложную задачу. В методологическом плане для ее решения интерес может представлять подход к формализации и последующей практической реализации процессов автоматизированного управления на основе парадигмы процессов оперативного (оперативно-технического и технологического) управления инфотелекоммуникациями как комплексного сочетания использования механизмов и средств программного и событийного управления.

Данная парадигма предполагает ряд базовых положений, основными из которых являются следующие:

1) Система управления имеет многоуровневую древовидную архитектуру, которую образуют:

- органы управления, должностные лица которых решают задачи планирования применения инфотелекоммуникационной сети, ее фрагментов (зон) и средств;
- пункты управления различных уровней (системы, зоны, объекта), на которых должностные лица решают задачи оперативного управления – оперативно-технического на сетевом уровне и технологического – на объектовом (узловом);
- средства автоматизированного управления инфотелекоммуникациями объектового (узлового) и сетевого уровней – унифицированные и частные (для отдельных типов сетей и / или их компонентов);
- собственно средства инфотелекоммуникаций с встроенными агентами мониторинга и управления (сетевые элементы).

2) Результатом планирования, осуществляемого как реакция на определенные внешние и внутренние события, является иерархия информационных компонентов следующих видов: программ, планов, шаблонов поведения, сценариев автоматического реагирования. Программы определяют перспективную инфраструктурную динамику развития и применения инфотелекоммуникационной системы (ИТКС), реализуемую через планы, в свою очередь задающие целевое состояние ИТКС и/или целевые мероприятия / плановые действия различного характера. Следствием планов являются шаблоны поведения должностных лиц в различных ситуациях и в общем случае допускающие вариантность выполнения в зависимости от различных условий (в том числе результатов выполнения предыдущих действий, параметров функционирования управляемых объектов и т.д.), а также сценарии автоматического реагирования, которые должны автоматически выполняться в определенных (заданных) условиях средствами управления, взаимодействующими с сетевыми элементами, или непосредственно агентами управления сетевых элементов. Сценарии также могут допускать вариантность выполнения с учетом обратной связи с сетевыми элементами.

3) Система управления способна фиксировать различные события – внутренние и внешние, первичные и производные. В частности, выполнение, не выполнение или не своевременное выполнение запланированного действия порождают события. Кроме того, агенты мониторинга и управления сетевых элементов также могут порождать события, связанные с их функционированием. Любые изменения в системе программ, планов, шаблонов и сценариев тоже трактуются как события. На любое событие следует реакция – на уровнях сценариев, шаблонов, планов и программ, связанные с их выполнением и / или коррекцией.

4) Можно условно считать, что в системе управления существуют два коррелированных потока – поток программного управления и поток событий, в силу ряда факторов имеющих в общем случае неопределенный характер. Истоками и стоками потоков с одной стороны являются процессы функционирования сетевых элементов, а с другой – процессы планирования применения.

5) Реализация указанных выше потоков требует наличия контрольно-организующей системы, основными функциональными компонентами которой являются распределенные по системе управления и взаимодействующими между собой компоненты типа «координатор», «диспетчер», «менеджер», «контроллер». Каждый из них играет определенную роль в реализации потоков программного управления, порождения событий, реакции на них.

Описанный выше подход дает возможность развития автоматизации управления инфотелекоммуникациями в направлениях унификации, интеграции, интеллектуализации и «роботизации» со смещением методологического аппарата их построения в сторону семиотических систем, знаковой основой которых являются элементы программного управления и событийные производные рефлексивного характера.

Шерстюк М.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»

МЕТОД ХРАНЕНИЯ ФАКТОГРАФИЧЕСКИХ ДАННЫХ В РЕЛЯЦИОННЫХ ТАБЛИЦАХ

Фактографическими данными, как правило, являются сведения, для которых характерны следующие признаки:

- они описывают происходящие в общей системе действия, т. е. имеют две составляющие — момент времени возникновения события и субъект направленности действия;
- наличие общей структурной составляющий в данных, т. е. общих инвариантных признаков в составе данных, которые могут отличаться только по значениям;
- потребность в анализе данных для каких-либо практических целей, к примеру, для выработки подкрепленных исследованиями управленческих решений, либо для лучшего понимания происходящих в системе процессов;
- большой объем данных, который необходимо хранить достаточно продолжительное время, либо вовсе выгружать в архивные хранилища.

В связи с особенностями структуры фактографических данных, для их хранения необходимо проектировать специальное информационное хранилище (ИХ). Применительно к реляционным базам данных основными признаками ИХ для фактографических сведений являются следующие особенности:

- необходимо использовать как можно меньше связей по внешним ключам между таблицами;
- БД ИХ должны быть построена по «второй нормальной форме»;
- динамическая составляющая фактографических данных по возможности должна храниться совместно с общей инвариантной частью;
- необходимо наличие индексов для всех атомарных свойств, описывающих фактографические данные;
- первичный ключ для хранения фактографических данных должен быть простым и надежным, например, момент времени занесения записи в таблицу с точностью до секунды с дополнительным порядковым номером, обеспечивающим уникальность каждой обработанной записи в рамках каждой секунды;
- должны быть правильно подобраны типы данных для всех атрибутов таблиц в ИХ в соответствии с возможным доменом каждой категории фактографических данных;
- периодически должна выполняться очистка журналов транзакций для уменьшения лишнего занимаемого ИХ места на жёстком диске.

Из всего вышеперечисленного следует, что для ИХ, как правило, подходит одна единственная правильно настроенная таблица для хранения фактографических данных. Динамическая составляющая фактографических данных может быть учтена с помощью специальных структур данных, характерных для иерархических БД, а именно — либо простые одноуровневые хешируемые пары ключ-значение (параллель со словарями и двумерными массивами в языках программирования), либо более сложные вложенные структуры данных, лучше всего описываемые форматом json (JavaScript Object Notation).

Шипицын Д. Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АКТУАЛЬНОСТЬ И ПРОБЛЕМАТИКА ВНЕДРЕНИЯ МЕХАНИЗМОВ ПРИОРИТИЗАЦИИ ПАКЕТНОГО ТРАФИКА В СТАЦИОНАРНЫХ СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

С развитием инфокоммуникационных технологий и появлением новых приложений и видов связи, например, видеоконференцсвязь (ВКС), распределенные базы данных, передача потокового видео высокого разрешения и других, к современным пакетным сетям передачи данных предъявляются все новые требования по обеспечению качества обслуживания. Не исключением стали и пакетные сети Вооруженных Сил (ВС).

Одним из совокупности средств, позволяющих обеспечить требуемое качество обслуживания для различных приложений, является внедрение механизмов приоритизации трафика. Наибольшее применение в современных пакетных сетях нашла дифференцированная модель обслуживания, которая дает возможность управления, манипуляции агрегированными потоками трафика, генерируемых различными приложениями в соответствии с заданными критериями качества обслуживания. Для этого весь сетевой трафик делится на определенные классы, с различным приоритетом обслуживания. Каждый агрегированный поток трафика от приложений со схожими требованиями к обеспечению качества обслуживания обрабатывается на основе класса, которому он принадлежит.

Выделяют четыре основных класса обслуживания: 1. негарантированная доставка (Best Effort). К трафику данного класса не предъявляются особые требования по обеспечению качества

обслуживания. Данные доставляются по возможности и с использованием имеющихся свободных ресурсов; 2. ускоренная доставка (Expedited Forwarding). Основным критерием данного класса является минимальная задержка. К приложениям данного класса можно отнести передачу речевого трафика реального времени через пакетные сети (Voice over IP - VoIP); 3. гарантированная доставка (Assured Forwarding). Позволяет организовать гарантированную доставку всех пакетов потока. Является оптимальным для приложений реального времени передачи потокового видео, например, видеоконференцсвязь и технология IPTV; 4. класс служебного трафика (Network Control). Данный класс необходим для передачи служебного трафика сетевых протоколов.

В современных пакетных сетях Вооруженных Сил назрела острая необходимость внедрения механизмов приоритизации пакетного трафика. Особенно это актуально для таких приложений как видеоконференцсвязь, речевой трафик реального времени и передача сверхсрочных сообщений.

Основными проблемами для внедрения технологии приоритизации пакетного трафика являются: необходимость согласования сетевых политик и конфигураций на всех узлах сети; распределенная структура стационарной сети военного назначения, разделенная на две основные части – сети военных городков построенных на базе узлов связи комплексного оснащения (УСКО) и сети объединения, построенной на основе VPN-соединений IP/MPLS ПАО «Ростелеком»; необходимость приоритизации зашифрованных сообщений.

Для решения задачи приоритизации зашифрованных сообщений необходима организация транслирования нужных заголовков оригинального пакета в заголовки транспортного пакета, который будет обрабатываться узлами магистральной сети. Для сбалансированного распределения ресурсов между классами трафика необходимо установить зависимости и пороговые значения для критериев качества обслуживания для каждого из классов.

Внедрение механизмов приоритизации пакетного трафика в сетях ВС, несомненно, представляется перспективным направлением, которое должно позволить повысить эффективность функционирования сети. Но есть ряд принципиальных проблем, которые должны быть решены для этого.

Широков В.В., Егоров С.С., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

МЕТОДОЛОГИЯ ПРИКЛАДНОГО ИСПОЛЬЗОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ

Операционные системы (ОС) являются важным компонентом информационных систем. Выявить прикладные преимущества применения конкретных операционных систем позволяет анализ их особенностей, преимуществ и ограничений.

Следует отметить особенности трех самых распространённых семейств операционных систем с точки зрения перспектив их будущего развития.

Операционные системы семейства Windows. Основными достоинствами данного семейства ОС являются огромное количество прикладного программного обеспечения, созданного под ОС семейства Windows, большое количество драйверов устройств, обеспечивающих сравнительно простое подключение оборудования различного типа. Основными недостатками ОС данного семейства является высокая цена, как на саму ОС, так и на большое количество прикладных программ. Кроме того, характеристики ОС по защите от несанкционированного доступа остаются на невысоком уровне.

Операционные системы семейства MacOS. Достоинствами ОС данного семейства является высокое качество программного обеспечения, а также высокая степень защиты объектов ОС от несанкционированного доступа. К недостаткам данного семейства ОС относятся высокая цена, а также ориентация на ограниченный круг аппаратных платформ.

Операционные системы семейств Linux. К достоинствам ОС данного семейства относятся высокая степень защиты объектов ОС от несанкционированного доступа, работа в многопользовательском режиме, высокая надежность. И очень важное достоинство – распространение на бесплатной основе. К основным недостаткам относятся трудности освоения, трудности подключения многих типов оборудования. Благодаря своим достоинствам ОС семейства Linuxполучают все большее распространение. Важно отметить, что ОС семейства Linuxи ОС семейства MacOSотносятся к классу Unix-подобных ОС, поддерживающих одни и те же стандарты прикладного программирования. Кроме того, многие ОС для мобильных устройств разрабатываются на основе ядра ОС Linux. Другой, существующей на сегодняшний день, тенденцией развития ОС является создание национальных ОС. Создание таких ОС обеспечивает информационную безопасность страны. Большинство российских разработок ОС основано на архитектуре Linux.

С учетом изложенных особенностей различных семейств ОС следует признать необходимым актуализацию прикладного использования операционных систем именно по их методологии построения, специфики, наличию достоинств и ограничению по недостаткам, что лежит в основе более глубоких принципов их построения и технологий применения.

Важное значение в принципах построения операционных систем имеет принцип декомпозиции операционной системы на слои, каждый из которых отвечает за выполнение определенной функции. Следует рассмотреть функции управления последовательным выполнением программ, управления параллельными процессами, управления памятью, управления коммуникациями, управления файлами и управления информацией.

Основное внимание уделено механизмам взаимодействия параллельных процессов с механизмами создания потоков, механизмами диспетчеризации, очереди потоков, средств синхронизации и взаимодействия путем обмена данными между параллельными потоками. С информационной точки зрения важное значение имеют принципы управления файлами и управления информацией, управления памятью, управления коммуникациями. Необходимо учитывать применимые технологии связывания на различных этапах жизненного цикла программы, статическое и динамическое связывание. С точки зрения информационных технологий управления: функции управления последовательным выполнением программ, управления параллельными процессами, механизмы взаимодействия параллельных процессов. В операционной системе важна возможность специфичного использования компонент системы управления файлами, реализации основных функций доступа к файлу, чтения из файла и записи в файл, управление доступом к объектам операционных систем. В зависимости от размерности решаемых задач и требований к оперативности их решения или работы в режиме реального времени следует учесть стратегии управления памятью и их ограниченность, обусловленную организацией вычислительных и управленческих процессов операционной системы. Только на основании оценки прикладных возможностей манипуляции структурами памяти выстраивается методология управления коммуникациями с организацией внутренних и внешних коммуникаций, концепций технологии клиент/сервер, процедур обратного вызова и поддержки коммуникационных протоколов сетевого и транспортного уровня.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Алексеев И.В., Зегжда П.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ВЫЯВЛЕНИЕ ЗАШИФРОВАННЫХ ИСПОЛНЯЕМЫХ ФАЙЛОВ НА ОСНОВЕ АНАЛИЗА ЭНТРОПИИ СЕКЦИЙ ИСПОЛНЯЕМЫХ ФАЙЛОВ ФОРМАТА PE32

Одним из способов маскирования вредоносных программ, предназначенных для повреждения информации, хранимой в компьютерной сети, скрытого использования компьютерных ресурсов или для другого воздействия, которое нарушает нормальные операции компьютеров или компьютерной сети, является шифрование части программы с помощью программ-шифраторов. Шифратор получает на вход исполняемый файл и преобразует его в зашифрованную версию, сохраняя его первоначальное поведение. В зашифрованный файл добавляется функция расшифрования, которая после выполнения передает управление исходному содержимому файла. Зашифрованная копия не содержит известной сигнатуры, поэтому она не обнаруживается антивирусными средствами, использующими сигнатурный анализ. Данный способ маскирования вредоносного программного обеспечения активно используется злоумышленниками.

Согласно положениям теории секретности Шеннона, ненадежность сообщения – это условная энтропия H(X|Y) открытого текста X при известном шифртексте Y. Нулевая ненадежность означает, что существует практически единственное значение ключа, удовлетворяющее заданному шифртексту. Следовательно, чем выше энтропия шифртекста, тем выше его надежность.

К зашифрованным данным предъявляется требование близости к случайным. У незашифрованных данных имеются в распределении плотностей выраженные отклонения, которые могут служить показателем неоднородности распределения байт в файле, а значит – показателем отсутствия зашифрованности. Для поиска зашифрованных (случайных) данных используются статистические тесты проверки качества случайных последовательностей, входящие в наборы тестов: NIST SP800-22, DIEHARD, тесты Кнута и другие. Статистические тесты являются эффективными, но в силу особенностей работы алгоритмов сжатия многие тесты на проверку свойств равномерно распределенной случайной последовательности сжатые форматы файлов проходят. Результативно применение большого количества тестов для оценки свойств последовательностей, однако это неприемлемо при проведении анализа данных специалистом в силу ограничения по времени.

Таким образом, существует проблема данных тестов в применении их для обнаружения потенциально вредоносных программ, использующих шифрование в качестве способа маскировки. Тесты зачастую определяют последовательность бит сжатых файлов как случайную, наравне с последовательностью бит зашифрованных файлов, что не удовлетворяет задаче по выявлению вирусов.

На основе энтропии можно делать вывод о равномерности распределения случайной последовательности. Значение энтропии у зашифрованного файла будет выше, следовательно, можно выбрать пороговое значение для обнаружения зашифрованного файла. Для определения порогового значения полученный файл необходимо разбить на секции в соответствии с заголовком исполняемого файла, вычислить энтропию каждой секции, умышленно зашифровать каждую секцию и повторно вычислить энтропию каждой зашифрованной секции. Затем необходимо вычислить разницу между двумя значениями энтропии в соответствии со спектральным статистическим тестом NIST и для полученной разницы посчитать функцию ошибок. Полученный результат чем ближе к 0, тем выше вероятность того, что последовательность зашифрована. Пороговое значение для определения границы выбирается эмпирическим путем, как правило, это 0.01 или 0.001.

При зашифровании уже зашифрованной секции данных, разница между двумя значениями энтропий будет минимальна, при зашифровании незашифрованной секции данных разница между двумя значениями энтропий будет максимальна. Энтропия сжатого файла в силу особенности работы алгоритмов сжатия по словарю всегда содержит некий разброс, который при подсчете дистанции покажет значение меньшее, чем зашифрованный файл, следовательно, при зашифровании сжатой секции данных разница между двумя энтропиями будет ближе к максимуму.

Предложенный метод позволяет повысить качественный уровень эвристических методов обнаружения вредоносных исполняемых программ, использующих шифрование в качестве средства маскировки. Оно применимо для пользовательских операционных систем семейства Windows в качестве средства обнаружения вредоносного программного обеспечения на основе анализа

исходного файла до этапа его запуска, а также может быть интегрировано в комплексное антивирусное решение.

Баранов С.Н., Тележкин А.М., Мустафин Н.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

УПРАВЛЕНИЕ РИСКАМИ В ПРОГРАММНЫХ ПРОЕКТАХ

Известны различные модели описания рисков в программных проектах, отражающие природу рисков, временные (событийные), вероятностные характеристики, возможности идентификации и управления, возможные последствия.

Модели управления рисками составляют важную часть в программных проектах, выполняемых в соответствии с моделями CMM, CMMI, SCRUM, и реализуются в рамках международных и корпоративных стандартов.

В практике управления программными проектами рассматриваются таксономия (классификация рисков – систематизация, сегментация, приоритезация, категоризация, консолидация, контролируемость, управляемость) для различных проектов, последствия проявления рисков, проактивные технологии реакции на риски.

Приводятся результаты анализа рисков, основанные на практике выполнения более 50-ти проектов разработки программных систем в промышленной организации-разработчике высококачественного программного обеспечения.

Башмаков А.В., Когтев А.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

УГРОЗЫ ПРОСЛУШИВАНИЯ И НЕГЛАСНОГО СЪЁМА ИНФОРМАЦИИ С МОБИЛЬНЫХ ТЕЛЕФОНОВ

В настоящее время мобильные устройства пользователей, все чаще используются для работы в корпоративных сетях и выполнения служебных задач. В связи с этим, в компаниях серьезное внимание уделяется защищенности мобильных устройств и тем угрозам, которые от них исходят.

В первую очередь угрозы вызваны большим количеством уязвимостей, выявляемых последнее время в операционных системах мобильных устройств, большая часть которых устарела, никогда не обновлялась и обновляться не будет.

Во-вторых, серьезную угрозу представляет уровень доступа к пользовательским данным, который обеспечивается мобильными ОС и ПО. Устанавливая практически любое приложение на мобильное устройство, мы соглашаемся с предоставлением ему многих прав доступа. По неизвестной причине приложениям необходимы данные и ресурсы мобильного телефона (фотокамера, микрофон, SMS, архив фотографий). При этом никто в точности не знает, как именно они этими данными и ресурсами распоряжаются. С большой вероятностью разработчики руководствуются благими намерениями и просят доступ тем устройствам и данным, без которых весь функционал ПО не будет реализован. Но если вдруг в таком приложении действительно окажется шпионская «закладка» или ошибка, из-за которых произойдёт утечка ваших данных, то этого никто не заметит: исходные тексты программ не публикуются, изучать их работу крайне затруднительно. Более того исследователями неоднократно выявлялось ПО, которое транслировало в сеть Интернет информацию, которая ей совершенно не нужна.

Нельзя забывать, что мобильные устройства и операционные системы (MS Windows или OS X, iOS или Android) имеют полный контроль над всеми данными, которые хранят, и всеми ресурсами, которыми управляют. Согласно материалам, обнародованным Эдвардом Сноуденом, шпионские закладки внедряются на самом низком уровне, то есть в электронных схемах.

Серьезную опасность представляет и большой спектр вредоносных программ, которые проникают даже в официальные магазины приложений производителей ОС и широко используются злоумышленниками для доступа к данным пользователей мобильных устройств, кражи денежных средств с привязанных банковских карт и многое другое.

Не стоит исключать и угрозы, специфичные самой организацией передачи информации от мобильных устройств по радиоканалу и через различные сети передачи данных. Среди них:

1. Возможность прослушивания разговоров, ведущихся по мобильным устройствам. Причем в настоящее время такими возможностями обладают не только спецслужбы, но и криминальные элементы. Для этого используются специальное ПО, устанавливаемое скрытно на мобильные устройства или устройства, образующие «виртуальную соту» или системы «IMSI-catcher». Это специальный аппарат-ретранслятор, обнаруживающий уникальный идентификатор SIM-карты абонента (IMSI). Является ложной базовой станции сети мобильной связи, которая маскируется под настоящую. Радиосигнал с неё мобильными телефонами пользователей воспринимается как легальный. Система получает возможность негласно контролировать входящий/исходящий трафик

мобильных телефонов, попавших в зону действия этой виртуальной соты, а также деактивировать включённую абонентом функцию шифрования сигнала.

2. Атаки на сеть SS7, позволяющие перехватывать данные абонента, а также его местоположение, из любой точки земного шара. Есть даже коммерческие решения, которые позволяют отслеживать любых абонентов по всему миру.

Актуальные угрозы, исходящие от использования мобильных устройств, необходимо учитывать при организации системы защиты корпоративной информации.

Белоусов Н.С.
Россия, г. Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПЕРСОНАЛЬНЫЕ ДАННЫЕ СОТРУДНИКОВ, ОБРАБАТЫВАЕМЫХ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСИТЕМАХ

Как мы знаем руководство предприятий при приёме возможных сотрудников на работу, собирает о них различные сведения. Такими сведениями в организациях не проводящими работу с государственной тайной являются: фамилия, имя, отчество, гражданство, дата рождения, номер страхового свидетельства, знание иностранных языков, данные свидетельства о постановке на учет в налоговый орган, данные об образовании (номер, серия диплома, год окончания), данные о приобретённых специальностях, семейное положение, данные о членах семьи (степень родства, ФИО, год рождения, паспортные данные, включая прописку и место рождения), фактическое место проживания, контактная информация, данные о военной обязанности, данные о текущей трудовой деятельности. Этот перечень сведений соответствует стандартизированной форме учёта кадров Т-2, утверждённой Постановлением №1 Госкомстата от 05.01.2004.

Основным документом контролирующим работу сбор данных с государственных служащих является Указ Президента РФ от 30 мая 2005 г. N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела». Некоторые из тех данных, которые позволяет собирать данный документ, относятся к категории общедоступных персональных данных, доступ к которым может быть предоставлен неограниченному кругу лиц с разрешения самого субъекта персональных данных согласно Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных». В набор данных из группы документов хранящихся в корпоративных сетях о сотрудниках входят: Фамилия, Имя, Отчество, Год, Место рождения. Однако сведения о субъекте персональных данных могут быть в любой время удалены из общедоступных источников при попадании туда, по требованию субъекта или по соответствующему решению суда, либо по решению уполномоченных государственных органов.

Однако, согласно согласно приказу ФСТЭК России №17 от 11 февраля 2013 года. Для обеспечения защиты информации содержащейся в государственных информационных системах, должны проводиться следующие мероприятия:

- аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- формирование требований к защите информации, содержащейся в информационной системе;
- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.
- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

Безопасность персональных данных при их обработке в информационных системах передачи данных осущевствляется путём исключения несанкционированного доступа, в том числе случайного, доступа к персональным данным, в следствии чего может произойти блокировка, изменение, уничтожение, распространение персональных данных. Данная задача по обеспечению требований безопасности персональных данных при их обработке в информационных системах персональных данных целиком и полностью возлагается на оператора персональных данных в данном случае на администраторов государственных корпоративных сетей.

В связи с этим оператор должен:

- своевременно проводить мероприятия, направленные в первую очередь на предотвращение несанкционированного доступа (далее НСД) к персональным данным и (или) передачи их лицам, не имеющим законного права доступа к такой информации;
- своевременно обнаруживать факты НСД к персональным данным;
- не допускать различные воздействия на технические средства автоматизированной обработки персональных данных, в результате которых может быть как-либо нарушено их функционирование;

– незамедлительно восстанавливать персональные данные, модифицированные и(или) уничтоженные вследствие несанкционированного доступа к ним;

– осуществлять постоянный контроль за обеспечением уровня защищенности персональных данных.

Таким образом информация используемая в государственных корпоративных сетях о сотрудниках является является персональными данными и нуждается в особом правовом режиме.

Бойченко О.В., Тупота Е.С.
Россия, г. Крым, Крымский федеральный университет имени В.И. Вернадского

ТЕХНОЛОГИИ DATA LEAK PREVENTION В СИСТЕМЕ ЗАЩИТЫ КОММЕРЧЕСКИХ ДАННЫХ

В отчете аналитического центра «InfoWatch», по результатам исследования утечек корпоративной информации, определенно 1505 случаев потери важных данных для предприятий (рост на 10% по сравнению с 2014 годом при 32% внешних обнаруженных проникновений).

В большинстве случаев атака осуществлена на массивы данных (клиентская база, база поставщиков, база посредников и т.д.). Кроме того, 8% эпизодов, связанных с потерей данных, являются проникновениями с несанкционированным доступом к информации.

Опыт показывает, что наиболее эффективно применение программно-аппаратных комплексов на основе DLP-технологий наряду с возможностью использования собственно программных средств.

Отдельной проблемой, наряду с внедрением программного комплекса, является необходимость эффективного функционирования аппаратного комплекса консоли централизованного управления DLP системой. Исследования определяют, что в настоящее время наиболее надежными комплексами являются системы таких мировых брэндов, как Hewlett-Packard, IBM, EMC, Dell и т.д.

Следует отметить, что такие системы строятся на анализе потока данных, которые функционируют внутри информационной системы (ИС).

Использование такого алгоритма при обнаружении потока утечки данных в системе приводит к немедленному срабатыванию активной компоненты DLP, и передача потока блокируется. При этом DLP-система проводит обязательный анализ данных, входящих в защищаемую систему, а выявление степени конфиденциальности информации и дальнейшее ее блокирование происходит, благодаря проведению аналитических операций по выявлению содержания пакетов. Однако следует отметить, что не все DLP-системы могут читать содержание передаваемого пакета данных, так как отдельным программным продуктам свойственно нахождение специальных маркеров, характерных для конфиденциальной информации, например таких, как гриф документа, мета-код, значение хэш-функций и т.д.

Анализируя основные приложения для обеспечения функционирования рассматриваемой системы, прежде всего следует выделить Websense Data Security Suite, Falcongaze SecureTower.

Так в программный продукт Websense Data Security Suite обеспечивает мониторинг на каналах передачи электронной почты, а также сообщений MS Exchange, HTTP, FTP, HTTPS. Система может отправлять уведомления администратору о факте передачи конфиденциальной информации и полностью блокировать нежелательные потоки. Так же в комплекте с системой представлен ряд готовых стандартных шаблонов и надстроек. Данное программное решение также позволяет разграничить доступ к информации, ее удалению и изменению. Для расширения функционала данной DLP системы рекомендуется использовать специализированные программы, такие как Data Endpoint, Data Monitor, Data Protect, Data Discover. Система является весьма простой во внедрении, так как имеет специальный мастер. Однако в данной системе отсутствует русификатор, что может затруднить внедрение в российских кампаниях.

Falcongaze SecureTower является отечественной разработкой, основанной на поиске конфиденциальной информации за счет ключевых слов, тег, подписей и т.д. Такой подход обеспечивает отслеживание трафика по всем необходимым каналам связи. Особенностью данного продукта является полная интеграция в среду Skype , что обеспечивает осуществление перехвата голосовых сообщений. Кроме того, система обеспечивает отслеживание работы сотрудников предприятия за счет функции периодического производства скриншотов экрана сотрудников. Система так же осуществляет контроль на уровне IP-адресов, создавая определенные карты посещения. Функционально структура Falcongaze SecureTower состоит из сервера перехвата трафика, сервера контроля рабочих станций и сервера обработки информации. Еще одним явным преимуществом данной системы является ее легкая масштабируемость, что является весьма актуальным для развивающихся компаний.

Таким образом, в результате проведенного исследования установлено, что эффективная деятельность современных предприятий не возможна без использования современных технологий защиты конфиденциальной информации, что обусловлено высоким уровнем утечек информации, прежде всего по внешним каналам.

Анализ показал, что наиболее эффективными методами защиты данных фирмы в таком случае является использование DLP-систем за счет высокого уровня мониторинга каналов утечки, возможности контроля периметра корпоративной ИС, а также доступной стоимости в установке.

Бойченко О.В, Дячук В.С.
Россия, г. Крым, Крымский федеральный университет имени В.И. Вернадского

СПОСОБЫ ЗАЩИТЫ ДАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Безопасность объектов электроэнергетики является одним из определяющих факторов полноценного и полноправного проживания граждан на территории Российской Федерации. Свидетельством этому являются недавние события в Республике Крым когда при вступлении в силу энергетической блокады полуострова в холодное время года (ноябрь 2015 – январь 2016 гг.) многие семьи оказались без отопления и полноценных условий проживания, учебные заведения прекратили работу, а лечебные учреждения не имели возможности оказывать свои услуги.

Ярким примером также является случай выведения электросети из строя, который произошел на предприятии «Прикарпатьеоблэнерго» 23 декабря 2015 года. Схема работы хакеров была тщательно спланирована и успешно реализована, что в следствии может привести к повторным атакам в сфере электроэнергетики на схожих объектах, например, подстанциях Республики Крым.

Приведенное утверждение обосновывает необходимость разработки комплекса мер, направленных на создание надежной системы защиты данных в информационных системах управления электроэнергетикой. Среди основных программных комплексов по реализации автоматизированных информационно-измерительных систем технического учёта электроэнергии (АСТУЭ) и автоматизированных систем коммерческого учета электроэнергии (АСКУЭ), прежде всего, целесообразно выделить ИС в энергосбытовой деятельности.

К таким ИС относятся программный комплекс «Энергия Альфа» (специализированный программный комплекс верхнего уровня АИИС КУЭ, разработанный ООО «Инженерный центр «ЭНЕРГОАДИТКОНТРОЛЬ»); АС контроля и учета энергоресурсов I-EMS; АС контроля и учёта энергоресурсов ФГУП "НПО им.С.А. Лавочкина"; АС учёта и реализации энергоресурсов «МЕГАБИЛЛИНГ», а также измерительная АС контроля и учета энергоресурсов (ИАСКУЭ) "Пульсар" и др.

Все вышеперечисленные программные комплексы назначены на выполнение таких задач, как:

1. Автоматизированный сбор данных по расходу электроэнергии, сбор мгновенных параметров сети, диагностических данных с измерительных устройств, устройств сьюра и передачи данных (УСПД) и с промежуточных серверов АИИС КУЭ;
2. Обеспечение дальнейшего хранения, отображения, обработки и анализа консолидированной информации в рамках коммерческого и технического учета электроэнергии на промышленных предприятиях и в организациях, поставляющих и потребляющих электрическую энергию.

Защита данных на объектах электроэнергетики, прежде всего должна осуществляться с учетом особенностей реализации и функционирования автоматизированных систем.

Так, например, «Энергия Альфа» работает на высокопроизводительной платформе баз данных ORACLE. I-EMS для хранения нормативно-справочной информации, а также данных по выработке и потреблению энергоресурсов используется Microsoft SQL Server. Обе указанные системы работают по принципу распределения рабочих мест и централизованном сборе данных по локальной сети. Здесь обязательным условием обеспечения информационной безопасности является настройка прав доступа специалистов к соответствующим автоматизированным рабочим местам (АРМ), а также наличие firewall, антивирусов и в некоторых случаях – шифрования передаваемой информации. К подобному классу систем также можно отнести и ИАСКУЭ "Пульсар", которая предполагает передачу данных на сервер коммерческого учета посредством сетей Internet, Ethernet, «витой пары», телефонного модема, GSM-модема, PLC-модема, радиомодема и GPRS-модема.

Центр сбора и обработки данных АСКУЭР ФГУП "НПО им. С.А. Лавочкина" включает в себя многопользовательское ПО АльфаЦЕНТР, которое устанавливается на сервере БД и АРМ. В случае данной АИС разработка всех ПО ведется внутри данной организации и являет угрозу несовместимости с прочими АИС данной области, некорректен способ передачи информации в иные учреждения – итоговые данные передаются на бумажных носителях.. Способ защиты здесь – заранее оговоренный метод шифрования информации, при котором передаваемая информация не может быть искажена, а полученная – недостоверна, а также автоматизация передачи информации не только внутри данного программного комплекса, но также и в учреждения учета и отчетности в части энергопотребления.

АСКУЭ / АСТУЭ «МЕГАБИЛЛИНГ» реализована в виде интернет-магазина коммунальных услуг www.mega-billing.ru. Служит в основном для оплаты услуг и отслеживания задолженностей. Основные методы защиты включают все, применяемые к вэб-сайтам.

Таким образом, средства и методы защиты данных при автоматизации процесса информационного обмена на объектах электроэнергетики основываются не на специфике передаваемой информации, а на особенностях реализации и функционирования информационных систем коммерческого и технического учета.

Башмаков А.В., Проноза А.А., Романов Е.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРИМЕНЕНИЕ ЭКОСИСТЕМЫ БОЛЬШИХ ДАННЫХ ПРИ ИССЛЕДОВАНИИ СОЦИАЛЬНЫХ СЕТЕЙ В ЦЕЛЯХ ВЫЯВЛЕНИЯ УГРОЗ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Социальные медиа, объединяющие в себе социальные сети, блоги, форумы, новостные площадки, сервисы обмена мультимедиа и т.п., являются неотъемлемой частью современного виртуального мира. Активные действия пользователей таких сервисов во многом обеспечивают наполнение Интернета уникальным контентом. Социальным сетям отводится особая роль в области производства контента – по данным Brand Analytics, в 2016 году в России социальные сети включили в себя 66% от общего числа активной (пишущей) аудитории.

Производимая пользователями социальных сетей информация в виде персональных страниц и тематических сообществ, а также отдельных постов, комментариев, «лайков» («likes») и т.д. (т.н. социальные данные, social data) находит широкий спектр применений вне социальных сетей. Ее обработкой занимаются не только маркетинговые компании, собирающие статистические данные и проводящие анализ пользовательских предпочтений, но и различные группы, манипулирующие общественным сознанием и призывающие к неправомерным действиям. Именно поэтому правоохранительным органам необходимо осуществлять мониторинг социальных сетей и включать в свое поле зрения авторов, осуществляющих подготовку и рассылку сообщений, создающих угрозу общественной безопасности или безопасности государства.

В общем, процесс мониторинга социальной сети может состоять из четырех этапов: 1) сбор данных; 2) фильтрация и кластеризация; 3) анализ, моделирование, предсказание; 4) выдача результатов, визуализация. Однако подходы к обработке потоков социальных данных отличаются от привычных методов обработки данных с использованием реляционных СУБД и языка запросов SQL. Количество ежедневно публикуемых записей исчисляется тысячами, при этом сами записи представляют из себя текст на естественном языке и могут включать в себя иной сложный для анализа контент – изображения, аудио и видео файлы, географические данные, вложения и т.п. Нетрудно увидеть, что данные, извлекаемые из социальных сетей, удовлетворяют всем признакам больших данных (bid data): большой объем (volume), высокая скорость возникновения (velocity) и отсутствие единой структуры (variety).

Таким образом, для организации процесса мониторинга социальных сетей необходима разработка комплексной архитектуры сбора, обработки и визуализации больших данных. Согласно Ю. Демченко и др., для построения экосистемы больших данных необходимо определить модели данных, процессы управления данными, разработать аналитические инструменты их обработки, создать вычислительную инфраструктуру и обеспечить ее безопасность.

В качестве предмета исследования мы предлагаем выделять такие единичные объекты как «пользователь», «сообщество» и «пост». Объекты «пользователь» и «сообщество» необходимы для идентификации автора сообщения и установления его связей. Для описания моделей данных целесообразно использовать вложенные наборы пар «ключ-значение». Так, например, объект «пост» может содержать пользовательский текст, изображение, набор комментариев, принадлежать объекту «пользователь» и входить в состав объекта «сообщество».

Управление данными заключается в распределенной загрузке сведений об объектах исследования или, если позволяет вычислительная инфраструктура, в создании «зеркала» социальной сети. Во избежание чрезмерных нагрузок на оборудование, управление данными может включать их предварительную обработку и фильтрацию. Примером фильтрации загружаемых объектов может быть поиск в тексте объекта ключевых слов или проверка вхождения одного объекта в состав другого.

Анализ загруженных объектов заключается в выделении автора объекта и установлении его социальных связей с другими пользователями (являются друзьями, состоят в одном сообществе, делают «репосты» (repost), оставляют комментарии и т.п.). На основе загруженной информации целесообразно подвергать анализу и самого автора объекта (психологическому, криминологическому и т.п.). Результаты анализа могут быть представлены, например, в виде графа социальных связей.

Вычислительная инфраструктура, отвечающая за сбор, обработку и отображение данных, полученных из социальных сетей, зависит от конкретной реализации. Следует отметить, что использование такой эффективной системы обработки больших данных, как Hadoop, и популярного NoSQL-хранилища MongoDB позволяет существенно снизить риски и затраты на оборудование по сравнению с использованием централизованных СУБД.

Мониторинг социальных медиа и, прежде всего, социальных сетей, даст возможность правоохранительным органам работать на опережение и предупреждать преступления, последствия которых могут оказать ощутимое влияние на функционирование всей государственной системы. Появление эффективных систем обработки больших данных делает эту возможность реальной.

Большакова Л.В., Дементьева А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

О ВЛИЯНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ФАКТОРОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РОССИИ

В настоящее время общеизвестны основные опасности, которые угрожают экономике России и росту экономического потенциала страны. Это, прежде всего, инфляция, низкие доходы населения, быстрый рост цен, выезд трудоспособного населения за границу, существование убыточных предприятий, нуждающихся в модернизации, ряд внешнеполитических и внутриполитических проблем, проблемы трудоустройства и т.д. Такое множество, всем понятных, достаточно естественных и лежащих на поверхности проблем, отодвигает на второй план проблемы информационно-психологических факторов культурной сферы. Проблемы, которые нельзя не учитывать, так как степень влияния их на экономическое состояние государства может оказаться, достаточно высокой. К таким проблемам культурной сферы можно отнести «зомбирование» людей через СМИ, отсутствие у населения собственной точки зрения, алкоголизация населения, отсутствие интересов в жизни, отсутствие уважения между людьми, взаимная агрессивность, кризис культуры, падение нравственности, «отупление» населения, подмена ценностей.

Однако, не стоит утверждать, что проблема кризиса культуры не затрагивается совсем. Это далеко не так. Сложность в том, что многие активисты и реформаторы лишь осуждают общественную деградацию и для того, чтобы привлечь наше внимание, они читают моральные проповеди, прежде всего, про наши обязанности, а реального анализа обстановки не производят. Поэтому актуальной, на наш взгляд, является задача исследования взаимосвязи уровня нашей жизни, то есть экономического потенциала страны, от культурного роста населения.

Такое исследование, проведенное с помощью метода экспертных оценок, позволило выявить наиболее значимые для экономики проблемные информационно-психологические факторы.

Результаты исследования позволили сделать вывод о том, что проблема снижения культурного уровня и его влияния на экономическую безопасность действительно существует. Дальнейшие исследования данной проблемы, тем самым, являются более чем целесообразными.

Большакова Л.В., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

МНОГОКРИТЕРИАЛЬНАЯ ОПТИМИЗАЦИЯ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Системы защиты информации имеют разные характеристики, по-разному действуют в различных ситуациях. Поэтому одной из задач информационной безопасности является задача принятия решения о выборе наилучшего варианта системы защиты информации в соответствии с имеющимся критерием. Однако на практике достаточно часто возникают задачи, в которых требуется принять решение, оптимальное не по одному, а сразу по нескольким критериям. Таким образом появляется задача многокритериальной оптимизации.

Перед применением какого-либо из методов многокритериальной оптимизации рекомендуется сократить число возможных вариантов решения. Такое сокращение возможно с применением принципа Парето, согласно которому из множества возможных вариантов решений могут быть убраны худшие. Оставшиеся наиболее эффективные варианты образуют для данной задачи множество Парето, на котором происходит дальнейшее решение задачи оптимизации.

Основными методами решения задачи многокритериальной оптимизации являются метод уступок, метод главного критерия и метод свертки. Каждый из этих методов имеет свои недостатки и преимущества. Выбор метода связан с конкретными условиями рассматриваемой проблемы.

Метод последовательных уступок состоит в упорядочении заданного множества критериев и дальнейшей последовательной оптимизации по каждому из них.

Метод главного критерия предполагает преобразование многокритериальной задачи в однокритериальную по следующему правилу. Из всех критериев выбирается самый важный, по которому происходит оптимизация, остальные критерии при этом оформляются в виде дополнительных ограничений. Сведение многокритериальной задачи к однокритериальной по методу свертки происходит с помощью введения некого обобщенного критерия, называемого аддитивной или мультипликативной сверткой. Для составления свертки для каждого критерия i определяют две величины:

- возможное значение критерия i для каждого варианта x;
- весовой коэффициент критерия i.

Возможные значения критерия предварительно нормируются, а весовые коэффициенты определяются после ранжирования критериев, например, с применением метода экспертных оценок.

Обобщенный показатель представляется либо в виде суммы произведений возможного значения критерия на его весовой коэффициент (аддитивная свертка), либо в виде суммы степенных функции (мультипликативная свертка). По значениям обобщенного показателя выбирают наилучший вариант системы защиты информации.

Браницкий А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

КОМБИНИРОВАННЫЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК НА ОСНОВЕ СИГНАТУРНОГО АНАЛИЗА И МЕТОДОВ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА

Одной из актуальных задач в области информационной безопасности является обнаружение атак в компьютерных сетях. В данной работе для решения этой задачи предлагается применять комбинированный подход, основанный на совместном использовании сигнатурного анализа и методов вычислительного интеллекта.

Целью настоящего исследования является снижение риска заражения и отказа компьютерных узлов за счет применения разработанных методов обнаружения и классификации сетевых атак. В условиях массового распространения и доступности в использовании готовых компьютерных решений для проведения сетевых атак эта проблема приобретает глобальный характер.

Для достижения данной цели необходимо решить ряд следующих задач:

1. Разработка системы обнаружения и классификации сетевых атак.
2. Генерация набора данных для проверки качества работы системы обнаружения и классификации сетевых атак.
3. Построение математических моделей для обнаружения и классификации сетевых атак.

Разработанная система обнаружения и классификации атак, которая построена с применением названных подходов, совмещает в себе несколько компонент. Первая часть представляет собой набор из нескольких клиентских сенсоров, установленных на контролируемых узлах в сети. Предназначением таких сенсоров является первичный сигнатурный анализ сетевых потоков как на уровне отдельных пакетов, так и на уровне сессий транспортного уровня, а также вычисление количественных и статистических параметров сетевого трафика. Вторая часть представлена серверным приложением, принимающим на входе зашифрованный поток данных, который содержит сформированный сенсорами набор сетевых атрибутов. Для обработки полученных данных используется интеллектуальное ядро классификации объектов. Данное ядро построено с применением биоподобных методов (методов вычислительного интеллекта), отдельные выходные результаты которых могут быть сгруппированы для выработки окончательного решения о классификации тестового объекта. Среди рассматриваемых методов для объединения нескольких базовых классификаторов в единый комитет решателей применяются следующие подходы: мажоритарный арбитр, арбитр на основе динамических областей компетентности, классификационное дерево и мета-классификатор на основе многоярусного обобщения.

За счет использования предложенных моделей и их гибридных аналогов предполагается повысить основные показатели обнаружения и классификации аномальных сетевых соединений.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Браницкий А.А., Коломеец М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РАЗРАБОТКА СИСТЕМЫ ВИЗУАЛИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ДИАГРАММЫ ВОРОНОГО

В настоящее время все большую популярность приобретает обеспечение информационной безопасности с использованием визуальной аналитики. При этом, актуально создание новых методов визуализации безопасности компьютерных сетей, которые могут эффективно отображать текущее состояние системы, тем самым обеспечивая быстрое принятие оператором решений.

Как правило, в большинстве существующих систем визуализации используются графовые структуры или матрицы для отображения топологии сети, и карты деревьев для отображения вложенности и отдельных метрик. При этом, данные методы обладают рядом недостатков. Например, графы не могут отображать большое количество метрик, а отображение при помощи ребер и вершин подвержено воздействию информационного шума. Матрицы могут отображать метрики связей, но не могут отображать метрики хостов. А карты деревьев могут применяться исключительно для иерархических сетей.

Таким образом, предлагается подход к отображению компьютерных сетей, который основан на частном случае диаграммы Вороного и который обладает рядом значительных преимуществ по сравнению с классическими методами визуализации. Предлагается отображать метрики хостов сети в виде ячеек, а их связи как соприкосновение соответствующих ячеек. Метрики хостов можно выражать при помощи цвета, прозрачности или размеров ячеек, а метрики связей при помощи цвета, прозрачности, толщины и длины ребра.

Также подход имеет возможность обеспечивать укладку диаграммы Вороного в фигуру произвольной формы, позволяя визуализировать подсеть как отдельную диаграмму Вороного внутри одной из ячеек общей диаграммы.

Алгоритм построения диаграммы Вороного с сохранением топологии компьютерной сети состоит из следующих шагов:

1. построение планарного графа;
2. построение выпуклой оболочки на основе вершин графа, и дополнение графа ребрами соответствующими выпуклой оболочке;
3. для каждой вершины выпуклой оболочки, добавление фантомных вершин и соединяющих их ребер удовлетворяющих следующим требованиям:

a) фантомная вершина должна располагаться на одной прямой с весовым центром графа и соответствующей вершиной выпуклой оболочки;

b) ребро, соединяющее фантомную вершину и вершину выпуклой оболочки должно сохранять планарность графа;

4. построение ограниченной триангуляции Делоне на основе созданного графа;
5. формирование ячеек-хостов на основе принципа взаимности триангуляции Делоне и диаграммы Вороного;
6. формирование разделителей на основе соотношения топологии графа и топологии диаграммы Вороного.

Работа выполнена при финансовой поддержке фонда содействия развитию малых форм предприятий в научно-технической сфере (договор № 9167ГУ/2015 от 24.12.2015).

Булгаков М.В., Чечулин А.А
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ МОДЕЛИРОВАНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В СИСТЕМАХ ЖЕЛЕЗНОДОРОЖНОГО ДВИЖЕНИЯ

В настоящее время все большую актуальность приобретают проблемы управления информационной безопасностью крупномасштабных распределенных систем. При этом, особое внимание уделяется задачам противодействия кибертерроризму в отношении критически важных инфраструктур, представителем которых являются российские железные дороги (РЖД).

Для исследования вопросов управления безопасностью РЖД, предлагается моделирование потенциальных угроз и событий при помощи макета железнодорожной сети на основе решений компании Piko. Предложенный подход способен обеспечить имитацию системы управления движением локомотивов. При этом, макет должен позволять проводить эксперименты с необходимым приближением к реальным условиям.

Разрабатываемый макет должен отражать все основные элементы железнодорожной инфраструктуры, которые могут стать целью атаки злоумышленника. Таким образом, был сформирован набор особо важных физических элементов железнодорожной системы, с точки зрения обеспечения ее безопасности: локомотивы, семафоры, стрелки, железнодорожные развязки, переезды, а также железнодорожные станции.

Для управления локомотивами и элементами железнодорожной инфраструктуры на аппаратном уровне, в качестве командной станции предлагается использовать контроллер Arduino с применением дополнительной схемы, позволяющей преобразовать двоичный код в ШИМ-сигнал (сигнал широтно-импульсной модуляции), передающийся по железнодорожной магистрали.

Для обеспечения передачи данных применяется протокол DCC, являющийся стандартом для моделей железных дорог. На основе данного макета может быть сформирована SCADA-система для отображения информации о состоянии элементов железнодорожной сети, а также диспетчерского управления системой железнодорожного движения в реальном времени.

Предполагается, что данный стенд позволит изучить возможные атаки и инциденты безопасности в системах диспетчеризации и управления железнодорожным движением.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Бурлов В.Г., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
СИНТЕЗ МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМ УЧРЕЖДЕНИЕМ С ИСПОЛЬЗОВАНИЕМ АНАЛИТИЧЕСКО-ДИНАМИЧЕСКОЙ МОДЕЛИ И ИНТЕРНЕТ ТЕХНОЛОГИЙ

В каждом высшем учебном заведении (ВУЗе), предприятии, в государственном учреждении есть лицо принимающее решение (ЛПР), которое формирует процессы обеспечения функционирования данного заведения. Основа формирования процесса управления – это решение ЛПР. ЛПР принимает решение на основе модели. Решение ЛПР должно, как содержать модель процесса, который он формирует (управляет), так и являться системой. Существует всего два подхода к разработке системы (модели). Это разработка на основе анализа и на основе синтеза. Для управления государственным учреждением необходимо формировать процессы с наперёд заданными свойствами. Это возможно только на основе знания закона построения и функционирования системы. Однако в известных публикациях такая закономерность не представлена. В данной работе мы выявили и сформулировали такой закон – закон сохранения целостности объекта и применили для синтеза модели решения человека для управления государственным учреждением. Математическая модель позволяет организовывать процесс управления ВУЗом, предприятием или государственным учреждением в интересах гарантированного достижения цели управления с использованием интернет технологий или без них.

В основе деятельности, как руководителя государственного учреждения, так и специалиста по управлению лежит решение человека. Человек осуществляет свою деятельность на основе модели. Поэтому для осуществление деятельности адекватной высшему учебному заведению необходимо располагать адекватной математической моделью решения человека. Сложилась интересная ситуация – в публикациях по выработке управленческого решения утверждается, что построить математическую модель решения человека весьма проблематично, если не сказать, что нельзя. А в публикациях представлены только результаты обоснования решения, но не модель самого решения! Но без математической модели решения весьма сложно гарантировать достижения цели управления государственной организации. Такая же ситуация и с построением системы обеспечения государственного учреждения, так как отсутствует критерий синтеза правильно построенной системы. Данная совокупность факторов определяет актуальность проводимой в данном направлении работы. А целью является выбор и обоснование условия гарантированного достижения цели управления на основе синтеза математической модели решения.

В процессе деятельности по управлению организацией очень часто возникает ситуация, когда результаты принимаемых решений не оправдывают ожидание человека. Для формирования условий, гарантирующих достижения цели деятельности используется естественно - научный подход к управлению государственным учреждением.

В целом, работе предложен метод управления государственным учреждением с использованием интернет технологий. Синтез системы управления государственного учреждения на основе системы дифференциальных уравнений позволит реализовывать гарантированный подход к управлению данной организации. Модель управления, в частности предложенных состояний, можно будет далее усложнять, введением дополнительных обратных связей и с учётом других условий.

Бухарметов М.Р., Ныркov А.П.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
О БЕЗОПАСНОСТИ КАНАЛОВ СВЯЗИ СИСТЕМ МОНИТОРИНГА ВОДНОГО ТРАНСПОРТА

На сегодняшний день одной из основных задач на отечественном водном транспорте остается обеспечение безопасности эффективных мониторинговых систем и систем безопасности судоходства в целом, как при смешанном плавании («река-море»), так и на внутренних водных путях России.

Для решения подобных задач необходимо создать профессиональную, целостную, комплексную систему, которая способна обеспечить гарантированную, надежную передачу навигационных данных от терминалов ГЛОНАСС в центры оперативного управления и диспетчерские пункты, которые проводят мониторинг и осуществляют контроль на водном внутреннем транспорте.

Такая комплексная система предназначена как для автоматизации различных процессов для управления и контроля, так и для обеспечения безопасности работающего на водных путях персонала и пассажиров, передвигающихся водным транспортом. Спутники ГЛОНАСС/GPS и различных контрольно-измерительные датчики осуществляют постоянный контроль текущего местоположения судов, а также маршрута их передвижений. С помощью этой системы можно легко формировать рейсы, организовывать расписание движения судов, отражать все маршруты на графиках, в том числе и планируемые, составлять подробные отчеты по маршрутам движения, учитывая остановки и общее время в пути, а также вести архив происходящего и т.д. Тем самым системы такого класса подразумевают наряду с хранением большого количества разнородной информации, представляющую собой данные различных уровней конфиденциальности, обеспечивают также грамотную ее обработку.

Планируя внедрение подобной системы мониторинга ГЛОНАСС, нельзя допустить нарушения безопасности и целостности передаваемой информации, так как появляется вероятность искажений и считывание данных третьими лицами. Утечка данной информации может привести к серьезным последствиям, особенно если это касается транспортировки ценных или опасных грузов, а возможность отслеживать местоположение транспорта значительно упростит работу злоумышленникам.

Самыми уязвимыми с точки зрения безопасности остаются каналы связи – сети GSM и Интернет, по которым данные с бортового навигационного блока сначала передаются на телематический сервер, а затем – на рабочее место диспетчера. Действительно, эти каналы защищены от рядовых пользователей, но не от тех, кто располагает необходимыми программными и аппаратными средствами для перехвата, а также желанием получить доступ к искомой информации.

Чтобы не допустить таких попыток, в современных системах мониторинга водного транспорта следует предусмотреть механизмы защиты данных. Так криптографические средства помогут обеспечить безопасность при передаче данных, сводя к нулю вероятность перехвата сообщения, и последующую его расшифровку, а механизмы стеганографии и электронной цифровой подписи позволят сохранить целостность передаваемых данных. Взаимная проверка подлинности при аутентификации элементов системы мониторинга, исключит шанс третьих лиц получить несанкционированный доступ к информации на серверах, а автоматическое шифрование передаваемых данных в совокупности с контролем целостности данных надежно защитит циркулирующую в сети информацию от злоумышленников и исключит возможность целенаправленного искажения, фальсификации или подмены данных. Только в случае комплексного подхода к обеспечению информационной безопасности объектов системы мониторинга водного транспорта, информация, проходящая от бортового блока до рабочего места диспетчера, будет надежно защищенной от злоумышленников.

Винокурова А. И., Ермачкова В. И., Спивак А.И.
Россия, Санкт-Петербург, Университет ИТМО

ПРИМЕНЕНИЕ МОДЕЛЕЙ АТАК НА ОБЕЗЛИЧЕННЫЕ ДАННЫЕ В СИСТЕМЕ ЗАЩИТЫ БАЗ ДАННЫХ

В современном мире огромные объёмы информации хранятся в разного рода базах данных. Многие из таких баз нуждаются в системе защиты от неправомерных действий со стороны злоумышленников. Одной из составляющих такой системы может стать межсетевой экран, выступающий в роли посредника между запросами к базе данных и самими данными.

В результате проведенной работы были получены модели разнообразных атак, направленных на раскрытие конфиденциальности данных, и предложена концепция использования этих моделей для защиты баз данных. В качестве инструмента реализации данной концепции был выбран межсетевой экран.

В данной работе рассмотрена возможность применения разработанных нами моделей атак на обезличенные данные в качестве расширения функционала по противодействию такого рода атакам межсетевого экрана баз данных. На основе принципа действия триггеров существует возможность разработки правил межсетевого экрана, направленных на предотвращение получения злоумышленником конфиденциальных данных. Модели атак позволяют вывести характерные наборы действий злоумышленника, которые могут привести к успешной реализации этих атак. Благодаря этому при написании правил для межсетевого экрана можно добиться более устойчивой системы защиты данных, описав в них необходимые меры реагирования на подобные злонамеренные действия.

Домбровская Л.А., Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИСПОЛЬЗОВАНИЕ МИКРОПРОЦЕССОРОВ И КРИПТОГРАФИЧЕСКИХ МИКРОСХЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

В настоящее время информация представляет все большую и большую ценность. Сегодня есть множество способов защиты информациипри работе через интернет. Первый тип защиты – это средства аппаратного характера. Второй – программные меры защиты.Есть также средства защиты информации, которые относят к смешанному виду. Она сочетает в себе средства обоих типов. К такому тип защиты относятся, в частности, устройства аутентификации. Комбинация двух методов позволяет достигнуть максимального уровня безопасности.

Как известно, аутентификация может быть выполнена двумя основными способами – симметричным и асимметричным. Основное отличие между ними состоит в том, каким образом используются секретные ключи. Если и на стороне хоста, и на стороне клиента применяется один и тот же ключ, то аутентификация – симметричная. Если же используется математически связанная пара открытого и закрытого ключей, то аутентификация – асимметричная.

Асимметричная аутентификация также носит название инфраструктуры открытых ключей (или PKI). Она очень хорошо подходит под требования окружающего нас мира. Фактически Интернет является одним из главных пользователей PKI.

На практике столь же часто применяются комбинации симметричного и асимметричного подходов с их плюсами – скоростью работы симметричного и безопасностью асимметричного.

В статье рассмотрены в рамках симметричной аутентификации некоторые примеры организации дополнительного уровня защиты информации во встраиваемых системах на базе криптографических микросхем и микропроцессоров.

Симметричная аутентификация может быть реализована разными способами:

1.Схема«запрос – ответ» с хранением секретного ключа на стороне хоста.

Основные особенности:

- быстрый процесс симметричной аутентификации;
- защищенные криптографические микросхемы на обеих сторонах обеспечивают безопасное хранение секретных ключей.

2.Схема«фиксированный запрос – ответ» без хранения секретного ключа на стороне хоста.

Основные особенности:

- быстрый процесс симметричной аутентификации;
- не требуется безопасное хранение секретных ключей на стороне хоста.

3.Схема«фиксированный запрос – ответ» с промежуточным ключом и без хранения секретного ключа на стороне хоста.

Основные особенности:

- быстрый процесс симметричной аутентификации;
- не требуется безопасное хранение секретных ключей на стороне хоста.

4. Защита загружаемого кода при помощи симметричных ключей.

Основные особенности:

- можно создавать уникальные копии загрузок для каждого клиента путем привязки,например, к его серийному номеру;
- все загрузки будут верифицированными;
- пользователь может свободно разместить зашифрованный образ загружаемого кода в Сети.

5. Обмен симметричным сеансовым ключом (с криптографическими устройствами на обеих сторонах).

Основные особенности:

- ключи шифрования изменяются для каждого сеанса, что повышает уровень безопасности;
- очень простая, но защищенная методология;
- легко может быть реализовано с помощью микросхем.

6. Защита информационного канала между криптографическим устройством и микроконтроллером.

Основные особенности:

- обеспечивается проверка подлинности канала связи между микроконтроллером иаутентифицируемым устройством;
- функционал аппаратно реализован в любой микросхеме семейства CryptoAuthentication дляпростоты использования.

В настоящее время целесообразно для повышения надежности криптографической системы дополнительно использовать аппаратную поддержку,основанную на базе микроконтроллеров и криптографических микросхем.

Демидов Р.А., Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ПАРАЛЛЕЛИЗАЦИЯ ПОИСКА УЯЗВИМОСТЕЙ В БИНАРНОМ КОДЕ С ИСПОЛЬЗОВАНИЕМ КЛАСТЕРНЫХ ВЫЧИСЛЕНИЙ

Для задачи поиска уязвимостей широко применяется статический анализ бинарного кода. Его преимущества - возможность полного покрытия кода, возможность построения более удобного представления для машинного кода. Он позволяет обрабатывать все пути в графе передачи управления, а не только путь текущего выполнения программы, как в динамическом анализе. Непосредственный анализ немодифицированного кода имеет ряд проблем – отладочные ветки исполнения, необходимость учета семантики импортируемых функций, контроль за изменениями памяти. Распространенным является предварительное преобразование кода в машинонезависимое промежуточное представление (IR, Intermediate Representation), над которым проводится дальнейший анализ для поиска уязвимостей разной природы. Промежуточное представление кода представляет собой разновидность SSA-представления, в котором каждой переменной значение присваивается лишь однажды. Одной ячейке памяти в бинарном коде соответствует несколько ее версий в промежуточном представлении; таким образом, присвоение переменной значения происходит только

один раз при её инициализации. Это сильно упрощает обратную трассировку программы. Такое представление кода возможно получить как из исходного кода, так и из его бинарного кода.

Текущие подходы к поиску уязвимостей в бинарном коде основаны на анализе путей исполнения в графе передачи управления. На каждом из путей, связывающем пользовательский вход с “интересным” участком кода, проверяется выполнимость условий возникновения уязвимости – записи в невалидную память при переполнении буфера, целочисленного переполнения переменной, и так далее. Однако не всегда рассматриваемый бинарный код представляет собой исполняемый файл – он может быть динамической библиотекой или набором связанных библиотек. т.е. кодом без определенного участка с пользовательскими данными. В этом случае на предмет уязвимости должны исследоваться отдельные функции библиотек – с предположением о том, что входные параметры могут быть любыми. Наличие уязвимых параметров у функции потенциально делает уязвимым код, использующий эту функцию при подключении библиотеки. Также возможен вариант, когда рассматривается код интерпретатора или виртуальной машины, как, например, виртуальная машина ActionScript в Adobe Flash, или виртуальная машина Java. В этом случае пользовательский вход представляет собой байт-код, т.е. обладает намного более сложной структурой, чем, например, файл изображения или музыки. Это влечет новые трудности для анализа путей в графе.

В нашем подходе предлагается осуществлять параллельную обработку путей в графе передачи управления. Вершинами такого графа являются однородные блоки машинного кода; ребрами - операции передачи управления между блоками. Разные узлы вычислительного кластера отвечают за разные части графа передачи управления искомой программы. Обработка кода происходит параллельно на соответствующих текущим блокам узлах кластера. Движение по коду осуществляется “в обратном направлении” – от потенциально уязвимых участков вверх к тем блокам, где осуществляется их вызов. Переменные пользовательского входа, либо те, значения которых мы не знаем на момент анализа функции, полагаются символьными (в зависимости от соглашения о вызове функции - значения параметров функции на стеке либо в регистрах). При движении по графу в обратном направлении формируется набор приводящих к уязвимости ограничений на эти символьные переменные и проверяется их выполнимость. В случае, если система ограничений внутри какой-то функции перестает быть выполнимой, функция является безопасной, и данный путь исключается из дальнейшего рассмотрения. Если же уязвимые ограничения выполнимы, функция обозначается уязвимой и путь продолжает обрабатываться – рассматриваются все ее вызовы в коде. При этом добавляются связывающие ограничения на переменные-аргументы функции (т.к. уязвимая функция вызывается с определенными на момент ее вызова параметрами). В случае с исполняемым файлом наш алгоритм возвращает уязвимые пути исполнения вместе со значениями параметров, приводящих к уязвимости. В случае с библиотеками алгоритм возвращает уязвимые функции в библиотеке, также с уязвимыми значениями параметров.

Предложенная методика в настоящий момент тестируется для поиска уязвимостей целочисленного переполнения в x86-бинарном коде. Реализация подхода использует дизассемблер IDA Pro в качестве источника кода. Алгоритм анализа путей реализован на языке Python. В качестве движка символьного исполнения используется фреймворк z3py.

Десницкий В.А., Александров В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

В работе предложен подход к разработке типовой модели нарушителя в системах Интернета вещей. Разработка модели нарушителя осуществляется на основе анализа существующих работ в предметной области информационно-телекоммуникационных систем Интернета вещей. Модель относится к классу аналитических моделей и специфицирует релевантные категории нарушителей информационной безопасности с указанием целей нарушителя, его возможностей и видов атакующих воздействий. В общем случае предполагается, что нарушитель имеет полный контроль над компонентами системой Интернета вещей, включая администраторские привилегии, и не имеет доступа к доверенному серверу подсистемы защиты Интернет вещей.

Проведение анализа систем Интернета вещей на предмет их подверженности следующим классам атакующих воздействий: (1) атаки обратной разработки («реверсинг»), направленные на локализацию и последующую модификацию важнейших функций и данных внутри ПО устройств; (2) атаки на окружение выполняющегося программного обеспечения с использованием модифицированных виртуальных машин, эмулятор устройств, отладчиков и средств трассировки, которые позволяют отслеживать и перехватывать библиотечные вызовы процедур, динамически изменять содержимое регистров процессора и стека вызовов и без прямого воздействия на исполняемый программный код; (3) атаки «клонирования устройств», представляющие собой

одновременное использование нарушителем двух физических экземпляров некоторого устройства системы – оригинального устройства и модифицированного.

При этом в рамках атаки клонирования использование оригинального устройства обеспечивает нарушителя функционалом системы, предназначенным для легитимных пользователей, тогда как второй экземпляр устройства используется нарушителей для осуществления на него атакующих воздействий. Фильтрация исходящего трафика модифицированного устройства делает его фактически «невидимым» в системе и, в частности, для подсистемы защиты. В результате весь входящий трафик оригинального экземпляра устройства дублируется и отсылается также на модифицированный экземпляр для обеспечения возможностей его функционирования в системе.

Модель включает также атаки, направленные на истощение энергоресурсов устройства с целью его отключения или увеличения значений среднего энергопотребления его модулей. При этом действия нарушителя будут непосредственно зависеть от разновидности реализуемой атаки. В общем случае возможно увеличение энергопотребления модулей устройства при помощи изменения режима работы устройства при его принудительном переводе из режима оптимальной работы (режима сна) в режим активной работы.

Проведение атаки на истощение энергоресурсов имеет смысл в случае важности работоспособности устройства, на которое идет атака. Если это устройство можно быстро заменить, подключить к сети электропитания, или его функционирование не выполняет критически важных задач, то такая атака окажется нецелесообразной. Отметим также, что атака может проводиться без прямого контакта нарушителя с целевым устройством – через сеть Интернет, либо с использованием беспроводных коммуникационных интерфейсов устройства. Во втором случае ограничения на удаленность нарушителя от устройства для проведения атаки будет зависеть от диапазона частот волн, используемых для беспроводной связи, и силы раздающей антенны у нарушителя. К минимальным навыкам злоумышленника, для проведения подобной атаки, можно отнести базовые знания операционных систем семейства Linux и возможность воспроизведения руководств, доступных в сети Интернет без необходимости привлечения специализированных аппаратных средств.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-37-50035, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Десницкий В.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МЕТОДИКИ ВЕРИФИКАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

В работе предложены методики верификация информационных потоков в информационно-телекоммуникационных системах Интернета вещей на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы и на основе анализа политик безопасности с использованием знаний о конфликтах сетевых информационных потоков. В рамках топологического анализа строится ориентированный граф, определяющий сетевые соединения между устройствами системы, и оцениваются различные пути в графе с точки зрения информационной безопасности. В рамках подхода, основанного на политиках безопасности, информационные потоки описываются с применение формальных средств спецификации и анализируются на предмет наличия противоречий между ними.

В рамках методики верификации на основе топологического анализа производится выявление всех компонентов, которые лежат между двумя выбранными вершинами графа, как правило, между источником данных с высоким уровнем защищенности и вершиной с низким уровнем защищенности. Подобный анализ используется для определения периметра защиты или критически важного сегмента системы для того, чтобы оперативно устранить незащищенные компоненты системы или повысить их защищенность. В общем случае нахождение всех путей между двумя заданными вершинами в графе является задачей класса NP, поэтому для систем Интернета вещей с большим числом задействованных устройств, сенсоров и соединений между ними, поэтому для анализа таких систем применяются различные стратегии перебора в том числе на основе стратегии «разделяй и властвуй».

Когда пути в графе найдены, анализируется каждый из них на предмет того, действительно ли он представляет угрозу безопасности системы. При этом для каждого из путей существует целый ряд возможных исходов такой оценки, в том числе: (1) подтверждается ожидаемое нормальное поведение системы при передачи информации с использованием данного пути; (2) в рамках данного пути проявляется некоторое ожидаемое заранее нежелательное свойство системы, подтверждающее наличие в системе известной проблемы защищенности; (3) нежелательность данного пути

выявляется непосредственно в процессе верификации системы и относится к некоторой неизвестной ранее администратору проблеме защищенности системы. Для сложных систем число анализируемых путей может быть значительным, причем возможно большое количество ошибок первого рода (false positives), что существенно усложняет процесс верификации. Возможным путем уменьшения количества ложных срабатываний является введение некоторой статической семантики в модель процесса верификации.

В рамках методики верификации на основе политик безопасности производится оценка защищенности системы Интернета вещей путем проверки корректности политики безопасности этой системы и определения уровня соответствия информационных потоков в реальной системе заданной политике. Верификации правил политики, описывающих информационные потоки, относится к методам статического анализа с использованием метода «проверки на модели» с использованием инструмента SPIN и языка PROMELA.

В процессе верификации входные данные преобразуются в единый внутренний формат на втором этапе, после этого строится общая модель системы для верификации правил разрешения/запрета информационных потоков, представленная в виде конечного автомата и инициализированная входными данными во внутреннем формате. Аномалии в модели выражены формальными утверждениями, нарушение которых приводит исследуемую систему в некорректное состояние. Затем общая модель для верификации правил разрешения/запрета информационных потоков верифицируется специальными программными средствами, реализующими метод «проверки на модели». В процессе верификации выявляются все некорректные состояния системы в соответствии с заданными правилами, и полученные результаты интерпретируются. В случае обнаружения аномалии, создается описание, содержащее ситуацию и информационный поток, приводящий к возникновению аномалии, а также тип такой аномалии.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-37-50035, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Дремов А.С., Павленко Е.Ю., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ПРИМЕНЕНИЕ МЕТОДОВ ДИНАМИЧЕСКОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СПАМА В СОЦИАЛЬНЫХ СЕТЯХ

Стремительное развитие мобильных технологий привело к росту популярности социальных сетей, предоставляющих пользователям разнообразный новостной контент, возможности для коммуникации друг с другом и для совершения покупок. Активное использование социальных сетей привлекло значительное количество злоумышленников, стремящихся использовать огромную пользовательскую аудиторию для распространения спама, который представляет собой массовую рассылку нежелательных сообщений, содержащих рекламу, ссылки на фишинговые сайты и т.д. Популярность рассылки спам-сообщений с использованием социальных сетей обусловлено следующими причинами:

- огромная база пользователей, которая может быть легко классифицирована по полу или возрасту;
- возникновение доверительных взаимоотношений как между отдельными пользователями, так и между группами пользователей;
- распределение базы пользователей по географическому и временному параметрам;
- компьютерная неграмотность большинства пользователей социальной сети;
- наличие программных интерфейсов (API) от разработчиков социальных сетей, которые могут быть использованы для автоматизации действий по рассылке спама.

Для решения описанной проблемы применяются классические методы машинного обучения, например, случайный лес (RandomForest), метод опорных векторов (SVM), наивный байесовский классификатор.

Однако данные методы обладают недостатком, заключающимся в их статичности, а, следовательно, в необходимости регулярной модификации классификаторов. Поскольку в социальных сетях поведение злоумышленников является динамическим (меняются методы распространения спама, признаки учетных записей, с которых распространяется спам), результаты построенного классификатора на новых данных с большой вероятностью будут ошибочными. Это потребует постоянно создавать тестовое множество признаков и повторять остальные шаги, что делает данные методы непригодными для выявления спама в социальных сетях. Временные изменения учитываются с помощью методов машинного обучения, обеспечивающих настройку параметров алгоритма каждый раз при добавлении нового объекта.

В результате классификатор обновляется и создавать новое множество данных не требуется. Данные методы относятся к классу так называемых методов динамического обучения.

В данной работе предлагается подход к обнаружению спама, в основе которого лежат алгоритмы динамического обучения, реализующие модификацию классификатора при добавлении новых данных в режиме реального времени. Данные для обнаружения спама предлагается разделять на две категории: параметры сообщения и параметры учетной записи – автора сообщения.

Параметры сообщения:

- наличие ссылок на сторонние ресурсы;
- длина сообщения;
- использование сервисов для сокращения длины ссылок;
- доля слов, входящих в словари спам-слов и т.д.

Параметры учетной записи автора:

- дата регистрации;
- число друзей;
- число подписчиков
- частота добавления новостей на страницу;
- число уникальных фотографий и т.д.

В алгоритмах динамического обучения каждому набору признаков ставится в соответствие специальная метка, после чего выполняется процедура извлечения признаков и формирования векторов, компонентами которых являются отобранные признаки. На основе полученных векторов и меток строится классификатор H_n. С течением времени в систему добавляются новые данные, которые могут содержать уже другие параметры сообщения или учетной записи автора. Обновление данных происходит итеративно в режиме реального времени, в результате на каждой итерации получается новый классификатор H_{n+1}.

Предложенный подход, в основе которого лежат динамические методы обучения, позволяет выявить спам в социальных сетях, с учетом постоянного изменения способов его распространения. Применение данного подхода позволит фильтровать вредоносный контент в социальных сетях и блокировать учетные записи пользователей, распространяющих его.

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ОЦЕНКА ЗАЩИЩЕННОСТИ НА ОСНОВЕ ГРАФОВ И ОТКРЫТЫХ СТАНДАРТОВ ДЛЯ СЕТЕЙ С МОБИЛЬНЫМИ КОМПОНЕНТАМИ

В настоящее время беспроводные сети используются повсеместно. Распространение мобильных технологий создает новые риски для компьютерных сетей, которые включают риски атак как против беспроводных каналов связи, так и против беспроводных клиентов (это могут быть мобильные или стационарные устройства). В то время как стационарные устройства, подключенные к беспроводной сети, еще можно контролировать, мобильные устройства могут подключаться и отключаться от сети, создавая таким образом дополнительные точки входа для атак, которые проконтролировать сложнее.

В данной работе предлагается методика оценки рисков компьютерных сетей с учетом мобильных компонентов. Отличительные особенности методики:

1) применение графов атак (узлы графа соответствуют шагам атакующего в сети, а дуги – связям между последовательно выполняемыми шагами) для моделирования возможных действий атакующего;

2) применение открытых стандартов для представления входных данных (таких как уязвимости, программно-аппаратное обеспечение компьютерной сети, средства защиты) и оценки уязвимостей системы;

3) применение открытых баз уязвимостей и шаблонов атак;

4) применение количественных метрик для оценки защищенности.

В работе рассматриваются отличительные черты беспроводных сетей и анализируются возможности их учета для оценки защищенности.

При этом выделяются такие компоненты сетей, как беспроводные точки доступа, беспроводные каналы связи и мобильные устройства.

Предлагается методика учета данных компонентов при моделировании атак и оценке рисков. В случае беспроводных точек доступа учитываются известные уязвимости программно-аппаратного обеспечения данных устройств, которые можно найти в открытых базах. Для учета атак на беспроводные каналы связи используются известные шаблоны атак и их характеристики (такие как сложность и стоимость реализации, необходимые пред и постусловия реализации и другие). Для учета атак с мобильных устройств вводится метрика, значение которой зависит от уровня контроля внешних подключений к сети.

Кроме того, предлагается ряд метрик для оценки защищенности сетей с мобильными компонентами, на основе которых вычисляется значение риска компрометации активов сети. Таким

образом, предлагаемая методика позволяет выявить слабые места компьютерной сети с мобильными компонентами.

Для экспериментальной оценки эффективности методики реализован программный прототип. Работа прототипа рассмотрена на примерах. Ведутся эксперименты по оценке соответствия результатов работы методики реальной ситуации по защищенности сети.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Ежгуров В.Н., Петров С.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

БАЗОВЫЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ МОБИЛЬНЫХ УСТРОЙСТВ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ НА БАЗЕ СИММЕТРИЧНЫХ И АСИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

В настоящее время количество мобильных устройств с дополнительной функциональностью приближается двум миллиардам. Их широкая распространенность таких во много раз увеличила объемы информации, хранящейся на мобильных устройствах. Почти все мобильные устройства, представленные на мировом рынке, работают под управлением трех операционных систем: Android (на данный момент последняя версия 7.0), iOS (на данный момент последняя версия 10.0) и Windows(phone,rt, 10).

Современные мобильные устройства зачастую содержат фунционал, схожий или с персональными компьютерами. Зачастую пользователи хранят на мобильных устройствах не просто файлы и данные, но и рабочие заметки или документы, которые могут стать объектом внимания злоумышленников.

В рамках противодействия несанкционированному доступу к конфиденциальной информации предлагается разработать программный продукт, основной функцией которого будет являться шифрование данных на мобильном устройстве. К данномк программному продукту следует предъявить следующие требования:

1. Скорость работы.
2. Возможность передачи защищённых (зашифрованных) файлов по открытым каналам, и возможность использовать эти файлы различных устройствах.
3. Удобство интерфейса для конечного пользователя.
4. Наличие встроенного файлового менеджера.
5. Интеграция с облачными сервисами.
6. Кроссплатформенность.
7. Отсутствие критически узких мест.
8. Возможность восстановления данных при гибели или утрате мобильного устройства.
9. Полное затирание исходного файла.
10. Организация хранилища паролей.

В рамках разработки такого программного продукта предполагается дополнить данный список требованиями, выявленными в результате исследования рынка существующих аналогов.

В качестве алгоритма шифрования предполагается сделать выбор между симметричными и ассиметричными алгоритмами. В симметричных алгоритмах используется один ключ для шифрования и расшифровки сообщения. При симметричном шифровании используется множество подстановок и перестановок исходных данных. В ассиметричных алгоритмах используются два ключа: секретный ключ для расшифровки сообщения и открытый ключ, который генерируется с использованием секретного ключа для шифрования сообщения. Использование ассиметричных алгоритмов шифрования является довольно затратным по скорости обработки данных и недостаточно гибким, однако их сложнее взломать.

Программный продукт будет реализовываться на языке программирования java. Причина использования данного языка программирования обосновывается его широкой распространенностью и возможностью создания кроссплатформенностью приложений.

Такой программный продукт, позволит хранить в зашифрованном виде информацию в сети и получать к ней доступ по мере необходимости. После реализации проекта предполагается перейти к созданию автоматизированной системы.

Ерисова А.Д.
Россия, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова

ИСТОРИЯ И МЕТОДЫ АУТЕНТИФИКАЦИИ

Прежде чем говорить о различных методах аутентификации, следует внести ясность в используемые понятия и определить, что такое аутентификация, и чем она отличается от таких схожих понятий, как идентификация и авторизация.

1. Идентификация человека, то есть определение его личности.

2. Аутентификация, которую также можно назвать проверкой подлинности.

3. Авторизация – предоставление доступа, на который лицо имеет право (или отказ в нем).

Из всех трех этапов наибольший интерес, особенно в рамках информационной безопасности, представляет второй. Не так сложно придумать способ опознать человека и не многим сложнее реализовать механизм, уверенно обеспечивающий или надежно отвергающий доступ. Но если человек решил обмануть систему и притворится кем-то другим, как мы можем разоблачить его?

Это можно сделать с помощью трех различных подходов, называемых факторами аутентификации:

1. Фактор знания. Это то, что может знать только проверяемый человек.

2. Фактор обладания. В этом случае используется некоторый предмет, которым обладает человек.

3. Биометрический фактор. Аутентификация, которая основывается на физических или психологических особенностях человека, которые являются уникальными для него одного и никогда не встретятся у другого человека.

Отпечатки пальцев. Повторяемость отпечатка одного пальца составляет 0,00001%, что соответствует двум людям с одинаковым отпечатком на 100 000 человек.

Рисунок радужной оболочки глаза. Обладает большей точностью. Теоретически, на 1078 человек будут только двое с одинаковым рисунком сетчатки.

Голос. При анализе используется спектральные и временные характеристики голоса человека, то есть его тембр и то, как быстро каждый конкретный звук сменяется на другой.

Характер ввода с клавиатуры, также называемый «клавиатурный почерк». В этом случае может быть учтена сила нажатия на клавиши, продолжительность их удержания, скорость письма, паузы между нажатиями клавиш.

Подпись. Цифровое устройство, проводящее аутентификацию выполненной от руки подписи, называется дигитайзером.

Поведение. Также называется поведенческой аутентификацией. В этом случае программа анализирует действия человека на определенном сервисе.

4. Фактор местоположения. При аутентификации по местоположению доступ может быть получен только в том случае, если объект находится в определенном месте или наоборот, блокируется из ряда других мест.

Двухфакторная (многофакторная) аутентификация – это эффективный способ существенного усиления защиты. При многофакторной аутентификации используется либо одновременная проверка с использованием двух или более факторов, либо последовательная эшелонированная аутентификация, каждая стадия которой реализуется посредством разных факторов.

Жуковский Е.В., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В БИНАРНОМ КОДЕ

Существующие подходы к поиску уязвимостей в бинарном коде можно разделить на три категории: методы статического анализа, динамического анализа и смешанные подходы, сочетающие статический и динамический анализ. Каждый из подходов имеет свои сильные и слабые стороны. Так использование методов статического анализа приводит к большому количеству ложных срабатываний и не позволяет определить конкретные входные значения, приводящие к эксплуатации найденной уязвимости. Динамические методы поиска уязвимостей, такие как фаззинг, позволяют определить, при каких входных значениях достигается уязвимый код, но невозможно обеспечить покрытие всего кода за приемлемое время.

К смешанным подходам, прежде всего, относится использование динамического символьного выполнения. Использование символьного выполнения, являющегося статическим подходом, позволяет определить зависимость промежуточных и выходных значений переменных от входных значений. Однако на практике у данного подхода есть существенное ограничение в применении, связанное с экспоненциальным ростом количества путей и отсутствием возможности решения всех полученных в ходе анализа уравнений. Для того чтобы решить данную проблему используется динамическое символьное выполнение, основанное на смешанном исполнении, когда символьной интерпретации подвергаются только некоторые переменные.

Так же использование динамического символьного выполнения позволяет осуществлять автоматическое формирование данных, приводящих к эксплуатации уязвимостей. Решение задачи автоматической генерации эксплойтов позволяет исключить из анализа неэксплуатируемые ошибки и тем самым сократить время анализа полученных результатов.

При реализации технологии поиска уязвимостей с использованием символьного выполнения необходимо решить несколько проблем, к решению которых различные исследователи подходят по-

разному. Попытки применения динамического символьного выполнения для решения задачи обнаружения уязвимостей были описаны ранее в нескольких работах, наиболее известными проектами в этой области являются BitBlaze, Mayhem, S2E, Angr и другие.

Современные средства поиска уязвимостей в бинарном коде применяют множество различных технологий для получения приемлемого результата анализа. Так, например, проект с открытым исходным кодом angr предусматривает возможность использования следующих техник: механизмы восстановления графа потока управления (Control Flow Graph), использование промежуточного представления кода (Intermediate Representation), анализ состояний переменных (Value-Set Analysis), выполняемый на каждом шаге исполнения программы, механизмы бинарной инструментации кода, технология динамического символьного выполнения, механизмы воспроизведения ошибки, механизмы генерации эксплойтов, технологии обхода механизмов противодействия эксплуатации и другие.

На основе существующих средств анализа бинарного кода было реализовано средство, осуществляющее поиск уязвимостей в программном обеспечении, сочетающее методы статического и динамического анализа.

Зегжда Д.П., Зегжда П.Д., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ПРОБЛЕМЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ В СЕТЯХ ТРАНСПОРТНЫХ СРЕДСТВ

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

Характерными особенностями перспективных сетей, в том числе сетей транспортных средств VANET (Vehicular Ad hoc Network) и мобильных сетей типа MANET (Mobile Ad hoc Network), являются максимальная децентрализация и топология с высокой степенью динамики изменений, что определяет необходимость решения новых проблем, в том числе автоматизации управления безопасностью, обеспечения безопасности передаваемых данных, высокой пропускной способности сетей при условии эффективной и безопасной динамической маршрутизации. С целью решения указанных проблем авторами предложено использование технологию программно-конфигурируемых сетей (ПКС, software defined networks, SDN).

Основные элементы управляющей системы сети VANET/MANET, построенной с использованием ПКС:

- контроллер ПКС – обеспечивает управление потоками данных и сегментацию сети VANET/MANET, установку и реализацию правил контроля доступа, мониторинг состояния устройств, трафика и сетевой статистики;
- узлы программно-конфигурируемой VANET/MANET – коммутаторы ПКС и мобильные сетевые терминалы – находятся под управлением контроллера SDN, осуществляя передачу сетевых пакетов и их обработку в соответствии с правилами, заданными контроллером SDN;
- облачная эластичная вычислительная система – выполнение ресурсозатратных вычислений (например, расчет, оценка и прогнозирование дорожной обстановки, реализация комплексных политик безопасности, фильтрация и анализ безопасности сетевого трафика)

Как программно-конфигурируемая сеть VANET/MANET может работать с учетом степени вовлеченности контроллера SDN в процесс управления:

- централизованный режим – контроллер (кластер контроллеров) SDN контролирует все потоки данных, передавая на узлы правила обработки трафика;
- распределенный режим – контроллер ПКС отсутствует, режим представляет оригинальную сеть VANET/MANET;
- гибридный режим – контроллер (кластер контроллеров) ПКС осуществляет гибкий контроль в любом сегменте сети (например, контроллер ПКС рассылает правила политики, которые определяют поведение узлов сети в целом, а узлы ПКС используют локальный интеллект для пересылки пакетов и обработки на уровне потоков).

Достигаемые преимущества использования технологии ПКС в мобильных децентрализованных сетях:

- масштабный мониторинг ситуации в сети. Контроллер ПКС может назначать потоки по определенным каналам или удалять их в зависимости от изменяющихся условий функционирования и кибербезопасности;
- динамическое разделение и группирование информационных потоков. В ПКС контроллер устанавливает правила потоков данных, чтобы эти данные достигали всех необходимых узлов. Таким образом, передача данных напоминает широковещательную рассылку, осуществляемую контроллером в отношении групп устройств (например, транспортным средствам подписчиков

информационных сервисов, транспортным средствам специальных служб полиции, медицинской помощи и т.п.).

– эластичные сетевые сервисы. Виртуализация транспортных сетей призвана обеспечить абстрактные логические сети на общих физических сетевых ресурсах. При этом достигается эластичность вычислительной мощности и эластичность сервисов управления безопасностью.

Зуров Е.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОЦЕНКА ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ЗЛОУМЫШЛЕННИКОМ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

Понятие скрытого канала передачи информации введено нормативно-методическими документами ФСТЭК России. Такие каналы образуются в результате использования традиционных каналов связи и специальных преобразований передаваемой информации, не относящихся к криптографическим. В частности, такие каналы могут быть организованы с использованием методов цифровой стеганографии.

Стеганография – это метод сокрытия (инкапсуляции) некоторых конфиденциальных сообщений в составе другой информации (файла, называемого контейнером) с целью скрытия факта передачи этих конфиденциальных сообщений по традиционным каналам связи.

Рассмотрим возможности злоумышленника, перед которым стоит задача передать защищаемую информацию за пределы автоматизированной системы. Будем исходить из предположений, что злоумышленник или разработанное им программное обеспечение имеют непосредственный доступ к защищаемой информации, но при этом у злоумышленника нет права передачи (вывода) защищаемой информации за пределы контролируемого периметра автоматизированной системы.

Тогда для реализации поставленной задачи злоумышленник может воспользоваться одним из классических методов цифровой стеганографии, называемым LSB. Суть метода заключается в следующем. В качестве контейнера выбирается файл формата BMP, в котором цвет каждого пикселя закодирован 3-мя байтами, соответствующими цветовому набору RGB. Каждый байт сообщения, подлежащего сокрытию, разбивается на 4 двухбитовых блока. Затем в некоторых байтах BMP-контейнера (по определенному правилу) осуществляется замена двух младших бит соответствующим блоком сообщения.

Извлечение сообщения из контейнера происходит по аналогичному алгоритму. Но может оказаться, что владельцу автоматизированной системы известна подобная уязвимость и им введён запрет на передачу файлов формата BMP, а также иных подобных форматов за пределы автоматизированной системы.

В таком случае злоумышленнику потребуется прибегнуть к методам текстовой стеганографии, которые характеризуются использованием в качестве контейнеров, файлов тестового формата. Например, для того, чтобы спрятать сообщение в русскоязычном текстовом файле, злоумышленник разбивает каждый байт исходного сообщения на биты, а затем начинает последовательно просматривать символы, содержащиеся в контейнере, на предмет их совпадения с такими символами, как: «а», «с», «е», «о», «р» и т.п., имеющими одинаковое отображение, как в русском, так и в английском алфавите. Замена таких символов с русского на английский производится в том случае, если соответствующий бит исходного сообщения равен «1». Если бит исходного сообщения равен «0», то замена символа не производится. Зная описанный алгоритм, извлечь исходный текст из контейнера также не составит труда.

Теперь следует перейти к вопросу: «Существуют ли методы выявления каналов скрытой передачи информации?». Известно, что имеющиеся на рынке системы защиты от утечки информации легко справляются с задачей выявления попыток передачи за пределы охраняемого периметра файлов, содержание которых является конфиденциальным или содержание которых невозможно распознать (зашифрованных файлов). Для выявления скрытых каналов передачи информации в систему защиты от утечки информации должны быть заложены соответствующие аналитические методы.

Подводя итоги, следует отметить, что гарантированно обеспечить защиту информации от её утечки через скрытые каналы передачи информации не представляется возможным. Можно лишь предложить некоторые рекомендации.

В автоматизированных системах, в которых обрабатываются сведения, составляющие государственную тайну, средствами межсетевого экранирования и средствами защиты от несанкционированного доступа должны быть заблокированы все информационные потоки, позволяющие осуществить передачу данных во внешние (незащищённые) автоматизированные системы.

Владельцам автоматизированных систем, в которых обрабатываются сведения конфиденциального характера, следует разработать комплекс мер, направленных на выявление

скрытых каналов передачи информации. Такие меры, в том числе включают: ограничение перечня форматов файлов, разрешенных для передачи во внешние автоматизированные системы, разработку и использование специализированных программ, позволяющих выявлять аномальное содержание передаваемых файлов.

Иванов Д.В., Москвин Д.А., Овасапян Т.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ИССЛЕДОВАНИЕ МЕТОДОВ АУДИТА БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТ НА ОСНОВЕ ОБНАРУЖЕНИЯ АКТИВНЫХ УЗЛОВ IPV6-АДРЕНОГО ПРОСТРАНСТВА

К настоящему времени информационные системы прошли несколько эволюционных этапов, смена которых определялась главным образом техническим прогрессом и появлением новых технологических средств. По мере развития компьютерных и сетевых технологий список возможных атак, а также уязвимостей в системах расширяется. Таким образом, возникает необходимость в постоянном контроле состояния их защищенности. Иными словами, проведение аудита безопасности глобальной сети. Наиболее быстрым и эффективным методом является глобальное сканирование сети.

В сетях IPv4 глобальное сканирование обычно может занимать от нескольких часов до нескольких недель, в зависимости от глубины и способов сканирования. Однако на сегодняшний день резерв нераспределенных IPv4-адресов практически полностью израсходован. Ряд технологий, таких как NAT, прокси-серверы, внутрисетевая адресация, позволяющих уменьшить потребность в IPv4-адресах, все равно не способны полностью решить проблему исчерпывания. Расширение адресного пространства за счет перехода на протокол IPv6 является единственным доступным долговременным решением проблемы дефицита IP-адресов.

Несмотря на то, что предназначение протоколов IPv4 и IPv6 остается одинаковым и заключается в адресации узлов сети Интернет, внутреннее устройство протоколов значительно различается. Одним из самых значимых, с точки зрения глобального аудита, отличий является изменение размера IP-адреса с 32 до 128 бит. Для сравнения протокол IPv6 позволяет адресовать в 1028 раз больше хостов, чем IPv4. Данное изменение существенно осложняет процесс сканирования узлов.

Таким образом, встает необходимость в разработке новых подходов, позволяющих оптимизировать процесс обнаружения хостов в адресном пространстве IPv6.

Рассмотренные в работе подходы базируются на трех основных принципах.

– Искусственное сужение диапазона сканируемых адресов. Исследование принципов распределения IPv6-адресов провайдерами разного уровня, правил и закономерностей в формировании IPv6-адресов позволяет сузить диапазон адресов потенциально активных узлов. Использование этого подхода позволило сузить весь диапазон IPv6-адресов до подсетей, сравнимых по размеру с подсетями IPv4 адресного пространства класса A, сканирование которых занимает намного меньше времени.

– Ответное сканирование, после обращения целевой системы (“мимикрия”). Главным условием при использовании этого подхода является наличие плотного трафика от узлов сети Интернет. В качестве протокола, позволяющего обеспечить плотный поток входных пакетов, может быть использован, например, протокол синхронизации времени NTP, который настроен практически на любом компьютере. Суть подхода заключается в том, что активные узлы IPv6 адресного пространства, сами осуществляют подключение к серверу, который берет на себя роль общедоступного популярного сервера (например, NTP-сервера). Сервер успешно синхронизируют время ,обращающихся к нему хостов, и параллельно с этим собирает их IPv6-адреса.

– Поиск по смежным идентификаторам, позволяющим обнаружить хосты с IPv6-адресами. Одним из примеров смежных идентификаторов могут служить доменные имена. Поскольку доменные имена представлены в удобной для человека форме, то и перебирать их можно по заранее составленным словарям, что может значительно сократить время поиска активных узлов в сети Интернет.

Исследованные подходы, в данном виде, не способны обеспечить гарантированную точность и полноту полученных результатов, но, несмотря на это, являются первым шагом к созданию надежных механизмов для проведения глобального аудита защищенности IPv6 адресного пространства.

Ильченко Л.М. Зайцев С.И.
Российская Федерация, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова

ПОНЯТИЙНЫЙ АППАРАТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ

В XXI веке война огня и металла постепенно уходят на второй план, уступая место более жестокому способу завоевания – информационным войнам, которые являются способом покорения не сколько территории государства, сколько умов его граждан.

«Информационно-психологическая война» - термин, способствующий пониманию процессов, происходящих в политической жизни и геополитике, и отнесенный Генеральным секретарём ООН (A/56/164/Add/1 от 3.10.2001 года) к основным угрозам государству, обществу и личности. Был поставлен в один ряд со средствами несанкционированного доступа к конфиденциальной информации другого государства через информационную сферу.

В 1995 году Национальный Институт Обороны США в работе Мартина Либики предоставил классификацию информационно-психологических войн, составленную по ориентации и методам воздействия:

- Командно-управленческая, целью которой является прерывание связи меду подчиненными и командованием, атаки направлены исключительно на каналы связи и в случае успешной реализации должны раскоординировать подчиненных лишив их управления сверху;
- Психологическая – целью является обработка сознания населения, внедрение изначально чуждых идеалов и взглядов;
- Разведывательная война, сутью которой является сбор значимой информации;
- Хакерская – вирусные атаки направлены на сбои в работе связи;
- Экономическая – блокада коммерческих каналов и информационных потоков;
- Кибервойна – целью данного вида информационно-психологической войны является захват информации;
- Электронная – вывод из строя всех сетей, радиоузлов, сотовых вышек и электронных средств связи.

По праву, самой опасной и массовой принято считать психологическую войну, способную оказать воздействие как на отдельные социальные группы, так и на все общество в целом.

Словосочетание «информационно-психологическая война» пришло в нашу страну из США, а именно из словарей военных терминов и при дословном переводе приобретает значение информационного противоборства. На его суть необходимо смотреть через призму типичной прагматичной идеологии, которая заключается в направленности на ближайшую перспективу, но не на сиюминутные необходимости. В условиях информационно-психологических войн с помощью психологического воздействия происходит формирование в сознании, как общества в целом, так и политически влиятельных кругов в отдельности установки необходимой потенциальному агрессору.

Под термином «психологическое воздействие» понимается способ, либо комбинированные в группу способы оказания скрытого либо явного психологического принуждения с целью получения определенного идеологического, психологического либо социального мировосприятия, а также изменение эмоционального состояния, и «программирование» субъектов на определенный тип поведения.

Самым простым и часто встречающимся методом в информационной политики является анализ уже существующих информационных потоков, на основе которого и строится вектор дальнейшей деятельности. В таком случае информация выступает в качестве лишь еще одного ресурса на ряду с материально-технической базой, экономический базой и трудовыми ресурсами.

Наиболее действенным, но сложно реализуемым методом в сфере информационной политики является контроль информационных потоков, а именно их распределения и доведения определенной информации заранее намеченной целевой аудитории с целью катализировать запланированную реакцию и добиться заранее намеченных эффектов. В таком случае, информация перестает быть дополнительным ресурсом и становится инструментом достижения политических, экономических, и других целей, путем непосредственного воздействия на субъектов.

Факторами, влияющими на вызываемый резонанс в обществе тем или иным информационным потоком и влияющим на восприятие самой информации:

- Вид знаний, которые несет информационный поток;
- Вид коммуникации, который задает способы предоставления информационных потоков конечным субъектам;
- Вид субъектов, на которых и направлен информационный поток.

Основной особенностью информации, выступающей как средство воздействия на определенный пласт общества выступает её «субъектность», то есть направленность не на саму суть знаний, а на реакции и общественные настроения, которые в конечном итоге должна вызвать эта информация. Информационные потоки перестают быть обезличенными, они приобретают вполне конкретные черты суверена, реального участника политического, экономического либо социального процесса, который производит эти знания на основе анализа уже существующих информационных потоков и их переадресации на необходимую целевую аудиторию. В роли такого суверена может выступать, как вполне конкретный человек, обладающий определенной властью либо социальная группа.

Несмотря на высокий уровень осведомленности о степени социальной опасности информационно-психологического воздействия на общество, используемого в информационных войнах, многие вопросы требуют своего решения, как со стороны правового, так и научного подхода,

в частности, при рассмотрении информационно-психологической войны, как крайнего способа борьбы в политических конфликтах выделяют следующие проблемы:

– Отсутствие законодательной характеристики операций в сфере информационно-психологической войны;

– Отсутствие общепризнанного определения войн информационного характера, однозначно определяющих организационные формы информационно-психологического воздействия, объединяющие операции и методы, которые представляют наибольшую опасность для государства, общества и непосредственно субъектов;

– Отсутствие научных методик, концентрирующихся на способах организации внутренней структуры операций информационно-психологического воздействия различных уровней сложности и отталкивающихся от конечного числа определенных элементарных составляющих данного воздействия;

– Отсутствие методик распознавания информационно-психологических атак, отсутствие их систематизации, поэтапного структурирования, а также классификации по степени воздействия, по признакам, по методам реализации и направленности.

Феномен информационно-психологической войны проявился относительно недавно, причиной которого послужило множество факторов: глобализация мира, развитие технических средств, способствующих массовому распространению информации, существование глобального информационного пространства и т.д.

Поэтому проблема защиты в информационной войне — это проблема защиты знания и системных взаимосвязей. И, в первую очередь, защиты национальной системы просвещения (воспитания и образования).

Ильченко Л.М. Зайцев С.И.
Россия, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова

ОЦЕНКА ОПАСНОСТИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Угрозы могут иметь антропогенный, стихийный и техногенный характер. Источником антропогенных угроз является человек. Угрозы техногенной группы обусловлены объективными причинами, основанными на свойствах технических средств, а также несовершенстве программного обеспечения. Источником угроз стихийного характера являются природные явления.

Все угрозы, вне зависимости от характера могут быть направлены на программно-аппаратный комплекс (каналы связи, автоматизированные рабочие места, серверы, активное и пассивное сетевое оборудование, операционные системы и прикладное программное обеспечение), информацию (вне зависимости от ее характера: видовая информация, информация в виде логических структур, информация, циркулирующая в виде электрический, электромагнитных, оптических сигналов, акустическая информация и т.д.), персонал либо помещения.

Особенностью оценки опасности угроз безопасности информации, составляющей персональные данные (ПДн), является рассмотрение ущерба с точки зрения пользователя удостоверяющего центра (УЦ), а не со стороны упущенной прибыли или экономического ущерба для компании. Данная оценка определяется вербальным показателем опасности, имеющим три значения:

1. Низкая опасность – реализация угрозы влечет за собой минимальные негативные последствия для Пользователей УЦ.

2. Средняя опасность – в случае реализации угрозы могут возникнуть существенные негативные последствия для Пользователя УЦ.

3. Высокая опасность – реализация угрозы может привести к весьма значительным негативным последствиям для Пользователя УЦ.

При рассмотрении актуальных угроз безопасности персональных данных пользователей УЦ наибольшую опасность представляют угрозы антропогенного характера связанные с утечкой информации, содержащей ПДн, а именно: кража носителей информации, утечка видовой информации, утечка информации по техническим каналам связи, а также кража атрибутов и ключей доступа. Кроме того, существенный ущерб может повлечь за собой модификация операционной системы (ОС) и прикладного программного обеспечения (ПО). Данным категориям угроз присваивается высокий уровень опасности, так как при утечке информации пользователю УЦ может быть нанесен максимально возможный ущерб.

Среднюю опасность представляют угрозы, связанные с модификацией информации (вне зависимости от антропогенного, техногенного либо стихийного характера угрозы). Кроме того, среднюю опасность влечет исчезновение носителей информации.

Остальные угрозы можно условно отнести к категории, представляющей низкую опасность для пользователей УЦ, включающую в себя угрозы техногенного и стихийного характера. Такие, как модификация информации при ее передаче по каналам связи (КС), уничтожение ОС, уничтожение ПО, технических средств, помещений и персонала. А также угрозы антропогенного характера

связанные с кражей технических средств, уничтожением информации, ошибками сотрудников УЦ при эксплуатации программного обеспечения и технических средств, связанные с ошибками сотрудников при инсталляции прикладного программного обеспечения, уничтожением технических средств, носителей информации и прикладного ПО.

Нарушение нормальной работы системы также не влечет за собой никакого существенного ущерба для пользователей УЦ, что позволяет эту подгруппу угроз отнести к категории составляющих низкую опасность.

Под нарушением нормальной работы системы понимается нерациональное использование ресурсов системы, снижение скорости обработки информации, уменьшение пропускной способности КС, искусственное снижение объемов свободной оперативной памяти, объемов свободного дискового пространства, нарушение электропитания технических средств.

Необходимо также учитывать источник угроз, который может быть, как внутренним, так и внешним, что в целом не влияет на оценку опасности угроз, но имеет значение при оценке возможности и вероятности реализации угрозы, а следовательно, является одним из факторов при определении её актуальности.

Данную оценку необходимо учитывать при построении модели угроз персональных данных. На её основе базируется определение актуальности угроз.

Келесис Н.В.
Россия, Санкт-Петербург, Университет ИТМО

РАЗРАБОТКА МЕТОДА ПОИСКА WEB-УЯЗВИМОСТЕЙ ПРИ ПРОВЕДЕНИИ АУДИТА ЗАЩИЩЕННОСТИ

Проведение аудита защищенности становится все актуальней и востребованнее. Старт-ап проекты, банки, крупные предприятия, промышленные заводы заинтересованы в безопасности своих продуктов, так как эксплуатация уязвимостей злоумышленниками может нарушить или остановить бизнес-процесс. Чаще всего, злоумышленники, а также пентестеры исследуют ресурс методом Black Box, так как у них нет никакой информации об используемых технологиях, версии ПО и они взаимодействуют с системой только посредством внешнего интерфейса.

Целью работы является автоматизация процесса проведения аудита защищенности, путем получения первоначальных сведений о системе, проверки ресурсов на уязвимости и комбинирование найденных уязвимостей для повышения уровня критичности. Предложенный метод также позволить определить, сможет ли цепочка из некритичных уязвимостей повлиять на безопасность системы. В итоге, метод позволит аудитору ускорить процесс тестирования на проникновение, так как автоматизирует большую часть проверок.

Основными объектами исследования являются http-пакеты, передающиеся от клиента к серверу. В случаях, когда сервис подвержен к тем или иным уязвимостям, изменение значений параметров в пакете может привести к нарушению целостности, конфиденциальности, доступности данных. Предложенный метод находит точки входа в систему, фиксирует разницу между ответами сервера при легитимных и измененных пакетах и на основе алгоритма пытается скомбинировать уязвимости разных типов.

На сегодняшний день существует много сканеров, которыми пользуются аудиторы в процессе анализа защищенности. Но сканеры проверяют ресурс лишь по заложенной сигнатуре, которая очень редко приносит положительные результаты в связи с тем, что каждая система отличается от другой уникальной конфигурацией. В данной работе акцент ставится на разработку математической модели, позволяющая не только сканировать объект на уязвимости по сигнатурам, но и анализировать взаимодействие друг с другом отдельных уязвимостей. В ходе работы метода будет формироваться отчет о сканировании, по которому аудитор сможет увидеть, какие уязвимости были найдены в системе и на сколько критичнее являются скомбинированные уязвимости. Для определения критичности используется калькулятор CVSS, расположенный на сайте ФСТЭК. В отличие от обычного сканера, данный метод будет также проверять уязвимости в ролевой модели системы. Это позволит увидеть, может ли пользователь А совершать действия от имени пользователя Б.

На данный момент собрана база из типовых web-уязвимостей, продуман алгоритм сканирования, а основной задачей является адаптация математической модели к процессу комбинирования уязвимостей.

Коломеец М.В., Чечулин А.А., Копчак Я.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»

РАЗРАБОТКА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА СИСТЕМЫ ВИЗУАЛИЗАЦИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Существуют множество графических моделей для визуализации данных компьютерных сетей. Однако, каждая графическая модель может выполнять ограниченное множество классов задач.

Например, для визуализации топологий компьютерной сети могут использоваться графы, матрицы и карты деревьев (последние, в случае иерархической сети). Для визуализации сетевого трафика могут использоваться графики рассеивания и параллельные координаты. Для визуализации общего состояния (интегральной оценки) используются розы ветров, линейные графики и треугольные графики состояний. При этом, каждая модель, соответствующая определенному классу, эффективно отображают только часть аспектов общего представления. Так, для визуализации топологии небольших компьютерных сетей больше подходят графы, для больших и многосвязных компьютерных сетей – матрицы, а для иерархических – карты деревьев.

Общий графический интерфейс системы визуализации должен предоставлять возможность оператору работать одновременное с разными классами задач. Основным свойством такого интерфейса является возможность предоставления пользователю выбора графической модели в зависимости от входных данных и сценария использования системы.

Графические модели могут быть разделены на два класса по виду исходных данных: данные которых могут быть представлены в двухмерном виде (как правило это множество объектов и их свойства), и данные, которые могут быть представлены в трехмерном виде (множество объектов и их связей). На основе анализа входных данных, система визуализации формирует категории данных (паттерны), которые оператор, на свой выбор, связывает с метриками графических моделей. Как следствие, формируется информационная панель, состоящая только из тех графических моделей, которые соответствуют видам входных данных и пользовательским сценариям использования системы.

Таким образом, достигается необходимая достаточность графических моделей для визуального анализа данных безопасности при помощи графического интерфейса. В свою очередь, участие оператора в формировании паттернов позволяет избежать избыточности и как следствие избежать когнитивного диссонанса при анализе данных.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (контракт № 14.604.21.0137, уникальный идентификатор RFMEFI60414X0137).

Комашинский Н.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

АНАЛИЗ ПОДХОДОВ ДЛЯ ОБНАРУЖЕНИЯ ЦЕЛЕВЫХ АТАК

Современный мир цифровых технологий непосредственно связан с целевыми компьютерными атаками, которые стали серьезной угрозой для обычных компьютерных систем и критически важных объектов. Целевые атаки можно охарактеризовать как ориентированные на конкретный специальный объект. Такие типы атак обусловлены разными целями и часто причиняют значительно больший ущерб, чем обычные типичные атаки, так как при проведении целевых атак обычно используются уязвимости “нулевого дня”; часто они осуществляются для шпионажа или саботажа и проводятся экспертами в области информационных технологий. Для того чтобы лучше понять сложный характер целевых атак и отобразить специальные уязвимости на более широкую картину, их удобно смоделировать как многоступенчатый процесс. Целевая атака всегда предназначена для причинения ущерба конкретной организации.

Выделяется семь этапов реализации целевой атаки: (1) рекогносцировка – злоумышленники тщательно собирают информацию о компании, используя сетевое сканирование, отображение процедур, профилей пользователей для поиска соответствующих уязвимостей “нулевого дня”; (2) подбор инструментов – выбор комплексной тактики проникновения в сеть — иногда не напрямую, а через сети заказчиков, партнеров и поставщиков, также развитие целевого вредоносного ПО, установка вредоносных служб; (3) распространение через различные каналы передачи данных; (4) эксплуатация – дальнейшее развитие атаки с компрометацией более критичных узлов инфраструктуры с помощью перехваченных идентификационных данных, полномочий и вредоносного ПО или с использованием уязвимостей в архитектуре безопасности; (5) установка в систему – организация постоянного присутствия в целевой системе; (6) управление и контроль – возможность удаленного управления и контроля соединения; (7) целевая деятельность – включает в себя первичную задачу вредоносного ПО, такую как утечка данных и сокрытие следов активности.

Проблема распространения целевых атак становится серьёзной угрозой как для сетей коммерческих фирм, так и для сетей государственных организаций. Для эффективной борьбы с ними недостаточно применения только антивирусных средств, функционирующих непосредственно на ПЭВМ, но также необходима разработка и применение новых методик обнаружения активности бот-клиентов на уровне сети. Только комплексное применение этих средств поможет более эффективно решать задачу обеспечения безопасности конфиденциальной информации в корпоративной сети.

Для распознавания и анализа подозрительной активности или кода предлагается использовать четыре уровня подходов и средств анализа: (1) сбор информации; (2) статический анализ; (3) динамический анализ; (4) принятия решений.

Первый уровень отвечает за сбор информации с ключевых точек ИТ-инфраструктуры, необходимой для выполнения процесса непрерывного мониторинга. Ключевыми точками являются основные места ИТ-коммутации компании, такие как пограничные маршрутизаторы, сервера электронной почты, а также рабочие станции сотрудников. Таким образом собирается наиболее полный набор данных для эффективного анализа. На этом же уровне расположена система обнаружения вторжений, обеспечивающая контроль сетевых соединений.

Второй уровень отвечает за анализ данных, используя классические технологии детектирования и репутационные списки, что позволяет ему оперативно выносить вердикты.

Основная задача третьего уровня заключается в анализе поведения каждого объекта или URL. Абсолютно не важно, каким путем файл был доставлен, загружен пользователем или прислан вложением в электронном письме, он с одинаковым результатом будет доставлен на третий уровень для прохождения динамического анализа в “песочнице”. То же самое касается URL-адресов, после прохождения репутационной базы, они будут переданы на уровень динамического анализа.

К четвертому уровню относятся технологии принятия решений. Это заключительная экспертная ступень решения, отвечающая на главный вопрос – какая активность является опасной и относится ли она к целевой атаке.

В докладе предполагается использовать рассматриваемые уровни и подходы для сборки модели системы, способной справиться с обнаружением различных сценариев целевых атак. Предлагается модель обнаружения, основанная на семействе сенсоров, Snort-систем и надстройке над ними, реализующими третий и четвертый уровни анализа, а также технологиях больших данных.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Коротков В.В.
Россия. Санкт-Петербург. ГУМРФ им. адм. С.О. Макарова

ЕДИНЫЙ ПОДХОД К ИЗМЕРЕНИЯМ ПО КОНТРОЛЮ ЗАЩИЩЕННОСТИ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

В настоящее время по вопросам инструментального контроля защищенности защищаемых помещений от утечки речевой информации применяется большое разнообразие средств измерений (аналоговые и цифровые шумомеры, а также специализированные автоматизированные комплексы).

Практика проведения контроля защищенности на объектах информатизации показала разницу как в измерениях так и в подсчетах результатов. Отличия обусловлены различными возможностями контрольно-измерительной аппаратуры, недостатками строго оговоренными в руководящих документах условиями измерений и так называемым человеческим фактором, т.е. специалист проводит измерения на основании собственных представлений о методике измерений.

Предлагается четко оговаривать условия измерений. Иначе ставится под сомнение понятие проверки, контроля проведенных измерений и полученных кем-то результатов.

Котенко И.В., Ушаков И.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Санкт-Петербургский институт информатики и автоматизации РАН

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ ДЛЯ МОНИТОРИГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном мире наблюдается значительный рост объёмов и многообразия обрабатываемых данных, связанный, прежде всего с развитием информационных технологий и вычислительных способностей организаций. В связи с этим становится актуальной задача обработки огромных массивов информации, называемых большими данными, и последующего анализа трафика на предмет выявления угроз информационной безопасности. У термина "большие данные" нет строгого определения, однако принято считать, что это совокупность технологий, методов и инструментов, с помощью которых можно хранить и обрабатывать структурированные и неструктурированные огромные объемы данных, поступающие непрерывным потоком. Понятие Большие данные основывается на четырех V: Volume – объем обрабатываемых данных; Velocity – скорость обработки; Variety – разнообразие форматов данных; Value – ценность информации, извлеченной из обработанных данных.

В докладе рассматриваются результаты экспериментов по исследованию технологий больших данных, основанных на экосистеме Hadoop, Spark и Storm для задач мониторинга инцидентов информационной безопасности.

В ходе исследований были проведены эксперименты по мониторингу инцидентов информационной безопасности на базе созданного стенда. Экспериментальный стенд состоит из трех основных компонентов: (1) трафик от агентов, включающий источник данных в виде трафика с

зеркалируемых портов коммутатора Cisco Catalyst 2960; (2) вычислительный кластер Hadoop, состоящий из одного главного и шести рабочих узлов; (3) SIEM-система OSSIM, установленная на виртуальную машину в системе VMware vSphere.

Для обработки больших данных используется Apache Hadoop версии 2.6.0. Hadoop – набор свободно распространяемых программных средств с открытым исходным кодом, предназначенный для разработки и реализации программ, которые запускаются на кластерах из десятков, сотен или тысяч вычислительных узлов.

Принцип работы прототипа основан на обработке, загружаемых в HDFS, больших объемов данных, которая выполняется рабочими узлами на основе заранее выбранной функции. Главный узел объединяет результаты обработки блоков данных, и в заданном формате передает информацию SIEM-системе, которая анализирует ее, собирая статистику и применяя заданные правила безопасности. После анализа и корреляции, эта информация предоставляется оператору SIEM-системы в виде подробного отчета о событиях безопасности и выводах, полученных на основе их анализа.

В результате проведенных сравнительных тестов производительности системы, используя различные технологии построения больших данных, включая такие как Hadoop, Spark и Storm, были сделаны выводы об особенностях поточной обработки данных в системах Spark и Storm. Также был реализован функции, на основе которых выполняется обработка больших данных, настройка и тестирование работы SIEM-системы с воспроизведением сетевых атак и нарушений информационной безопасности.

В дальнейших исследованиях планируется в качестве источника информации для вычислительного кластера использовать эмулированную сеть SDN, а также внедрить в процесс обработки данных стоковое приложение Apache Kafka.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Левшун Д.С., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ЗАЩИЩЕННОЕ МЕЖКОНТРОЛЛЕРНОЕ ВЗАИМОДЕЙСТВИЕ НА БАЗЕ ПРОТОКОЛА I2C

Распространенность систем физической безопасности, а также критическая важность систем такого типа, обуславливает интерес злоумышленников и исследователей в области информационной безопасности к обнаружению брешей в их защите. Именно поэтому, все чаще обход систем физической безопасности становится одним из этапов сложных, многошаговых и растянутых во времени атак, происходящих на различных уровнях.

Одним из способов противодействия злоумышленникам, нацеленных на системы физической безопасности, является применение надежных протоколов для взаимодействия элементов данных систем. Под надежными протоколами здесь понимаются протоколы с применением шифрования передаваемых данных алгоритмами с высокой криптографической стойкостью, а также взаимной аутентификацией элементов систем.

Основные протоколы передачи данных, применяемые в системах физической безопасности, соответствуют только физическому и канальному уровням модели OSI, регламентируя параметры интерфейса передачи данных, максимальный объем передаваемых данных и диапазон адресов. Поэтому возникает необходимость в реализации дополнительного функционала поверх данных протоколов для их соответствия сетевому и транспортному уровням, что позволит расширить данные протоколы шифрованием и аутентификацией на сеансовом уровне (в соответствии с моделью OSI).

Рассмотрим предлагаемую реализацию защищенного межконтроллерного взаимодействия на базе протокола I2C.

Интерфейс данного протокола представляет собой последовательную шину данных, использующую две двунаправленные линии связи (SDA и SCL). При этом по линии SDA передаются данные, а по линии SCL передаются тактовые импульсы. Устройства, объединенные по протоколу I2C, являются или ведущими (master), или ведомыми (slave). Ведущее устройство генерирует тактовые импульсы, передаваемые по линии SCL, позволяя ведомым устройствам реагировать в зависимости от них. Максимальный объем передаваемых за один такт данных ограничен 8 битами. Всего к ведущему устройству может быть подключено до 112 ведомых устройств в рамках одного интерфейса I2C.

Таким образом, протокол I2C соответствует физическому и канальному уровням модели OSI. Для реализации надежного протокола передачи данных на базе протокола I2C, необходимо реализовать следующий функционал:

– динамическая адресация устройств на уровне, соответствующем сетевому уровню модели OSI;

– передача неограниченных объемов данных в рамках надежных сеансов связи на уровне, соответствующем транспортному уровню модели OSI;

– применение шифрования передаваемых данных и взаимной аутентификации устройств на уровне, соответствующем сеансовому уровню модели OSI.

Предполагается, что реализация данного функционала позволит организовать защищенное межконтроллерное взаимодействие на базе протокола I2C, при условии применения алгоритмов шифрования с высокой криптографической стойкостью, а также взаимной аутентификацией элементов систем физической безопасности.

Работа выполнена при финансовой поддержке фонда содействия развитию малых форм предприятий в научно-технической сфере (договор № 1327ГС1/22645 от 16.06.2016).

Левоневский Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РАСПОЗНАВАНИЕ ОБРАЗОВ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В настоящее время получило широкое распространение и стремительное развитие корпоративных информационных систем. Им присущи облачная архитектура, многомодальные технологии, реализация подхода интеллектуального пространства (Smart Space). Это позволяет не только повышать эффективность корпоративной среды, но и использовать современные технологии в области обеспечения безопасности предприятий.

Построение архитектуры безопасности предприятия предполагает решение, в частности, задач, связанных с идентификацией образов, как классов сущностей (человек, дверь, оружие и др.), экземпляров сущностей (определённый сотрудник или посторонний человек и т.п.), поведения (легитимная и подозрительная активность, попытка правонарушения).

Для идентификации движущихся объектов предлагается использовать усовершенствованный метод. Согласно ему применяется маска, единичные биты которой соответствуют пикселам, изменяющимся во времени. Программа накладывает маску на кадр, полученный из видеопотока, и вычисляет множество ключевых точек полученного изображения. После этого определяется ряд значений, представляющих собой относительные величины, характеризующие расположение ключевых точек относительно друг друга. Статистические распределения данных значений формируют дескриптор образа, хранящийся в базе данных.

Полученные распределения используются в качестве признаков идентификации при сравнении анализируемого изображения с эталонным путём вычисления среднеквадратического отклонения. Для этого выполняется сравнение распределений с ранее запомненными распределениями. На основе этого сравнения принимается решение о соответствии или несоответствии анализируемого изображения эталону. Это позволяет идентифицировать объект и отслеживать его действия в интеллектуальном пространстве. За счёт применения метода удаётся уменьшить влияние типовых помех (засветка, повреждение изображения) на результат распознавания. Это повышает надёжность способа распознавания изображений и расширяет сферу его применения.

Реализация предложенного метода предусматривает разработку: архитектуры данных о пользователях корпоративной информационной системы, позволяющую накапливать, хранить и обрабатывать информацию о поведении пользователя в течение всего времени взаимодействия с системой; сервисов, интегрированных в корпоративное интеллектуальное пространство. Среди них сервисы:

– хранения (программное обеспечение, предоставляющее доступ к реестру сотрудников и посетителей, библиотеке образов, базе знаний, содержащей описание сценариев поведения пользователей);

– сбора данных (компьютеры, получающие и хранящие данные с подключённых камер видеонаблюдения);

– анализа данных (программное обеспечение, анализирующее видеопоток и распознающее образы);

– оповещения (программное обеспечение, уведомляющее ответственных лиц о нештатных ситуациях);

– администрирования (программное обеспечение, предоставляющее аккредитованным лицам доступ к управлению системой сервисов безопасности).

Перечень таких сервисов и их возможности могут быть расширены за счёт использования возможностей, предоставляемых человеку интеллектуальным пространством. Например, можно обрабатывать сигналы RFID-идентификации, поступающие с пункта пропуска сотрудников предприятия (учитывая возможную ситуацию, когда используется пропуск другого человека), или анализировать коммуникации пользователя с корпоративной информационно-навигационной

системой. Такой подход позволит наиболее полно использовать ресурс корпоративного интеллектуального пространства в задаче обеспечения безопасности предприятия.

Лемец А.А., Павленко Е.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

АНАЛИЗ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ SSL PINNING В ПРИЛОЖЕНИЯХ ДЛЯ ОС GOOGLE ANDROID

Активное распространение информационных технологий привело к значительному увеличению объемов хранимой и передаваемой информации. При этом, часть информации является конфиденциальной, например, информация, содержащая пароль от аккаунта в социальной сети, информацию о банковском счете или коммерческую информацию. Поскольку сеть Интернет является открытым каналом связи, актуальной является задача обеспечения защищенности данных при передаче между конечными устройствами. Чаще всего для решения этой задачи применяются такие технологии, как SSL и TLS.

Использование криптографических протоколов SSL и TLS не является достаточным для защиты информации при передаче по сети Интернет, так как эти протоколы уязвимы к атаке типа MITM. По умолчанию, устанавливая SSL соединение, клиент проверяет, что сертификат сервера можно проследить до корневого сертификата (CA) доверенного центра сертификации, а также, что SSL сертификат соответствует запрошенному хосту. Таким образом, при использовании SSL существует зависимость от корневых сертификатов, и при компрометации любого из них, компрометируется почти весь SSL-трафик.

Все корневые сертификаты в ОС Google Android до версии 4.0 хранились в едином файле. Изменить его без root–прав было невозможно, а любое изменение требовало обновление ОС. С выходом версии 4.0 подход к работе с сертификатами изменился. Все сертификаты являются отдельными файлами и делятся на два типа: системные и пользовательские. Для установки пользовательского сертификата требуется загрузить его на SD-карту, а затем установить через настройки безопасности. Установив свой сертификат на устройство, можно расшифровывать SSL - трафик.

Решением вышеописанной проблемы, связанной с компрометацией корневого сертификата, стала технология SSL Pinning или Certificate pinning. Certificate pinning – это внедрение SSL сертификата, который используется на сервере, в код мобильного приложения. В этом случае приложение будет игнорировать хранилище сертификатов устройства, полагаясь только на свое хранилище и позволяя создать защищенное SSL соединение с хостом, подписанным только сертификатом, хранимым в самом приложении. Стоит отметить, что может внедряться не сам сертификат, а публичный ключ. Pinning SSL сертификата также позволяет создавать доверительное соединение с сервером, на котором установлен самоподписанный SSL сертификат, без необходимости устанавливать дополнительный сертификат на устройстве пользователя.

Скомпрометировать сертификат, добавленный в код самого приложения, не так легко, но возможно. Для этого существует два основных метода.

Первый метод основан на том, что злоумышленник декомпилирует приложение, вносит изменения в его исходный код, после чего вновь собирает. Однако после этого ему потребуется каким–то образом установить приложение на устройство пользователя (минуя официальный магазин), что является весьма непростой задачей.

Второй метод может быть применен только на устройствах с root–правами. Есть приложения, которые позволяют обойти SSL Pinning на устройстве, например, Android SSL Bypass. Обычно такие приложения используются исследователями для анализа сетевого трафика, но эти же подходы могут быть использованы и злоумышленниками во вредоносных программах.

Таким образом, certificate pinning обеспечивает повышение уровня безопасности, ведь с SSL сертификатом, внедренным в код, приложение становится независимым от хранилища сертификатов устройства. А чтобы обойти данную технологию, злоумышленнику требуется провести реверс-инжинирингприложения, что значительно сложнее установки корневого сертификата на устройство. Однако, ни один из рассматриваемых подходов не может обеспечить гарантированную защиту приложений, а лишь усложняет процесс получения доступа к сетевому трафику приложения, поэтому для защиты мобильных приложений для ОС Google Android целесообразно комбинировать certificate pinning другими методами защиты, такими как контроль целостности приложения, обфускация исходного кода и использование интерфейса JNI.

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, ООО «Газинформсервис»,
Республика Беларусь, г. Минск, УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД

СОСТОЯНИЕ ВОПРОСА ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИМПОРТОЗАМЕЩЕНИИ

Проблема импортозамещения, внимание к которой особенно усилилось в последнее время, получила широкое распространение на все сферы деятельности, в т.ч. и на область защиты информации. Следует заметить, что решения в области защиты информации всегда подчинялись определенным строгим «правилам игры», определенную часть которых формировал рынок, но большую часть – государственные регуляторы. Соответственно, при оценке текущей ситуации необходимо оценить, что было сделано в области защиты информации в РФ до настоящего времени, что делается сейчас и какие тенденции следует принять во внимание для успешной защиты от возможных негативных воздействий.

Можно предложить следующую формулировку исследуемой проблемы – является ли возможным решение глобальной проблемы защиты информации на современном уровне при решении локальных задач импортозамещения (технических, технологических, методических) и какие ключевые риски при этом возникают. Рассмотрение проблемы удобно начать с анализа главной стратегической цели – обеспечение технологического суверенитета в области информационной безопасности (ИБ). Понятие «ИБ» уместно применить по причине того, что представляется намного более общим, тем только практическая задача по защите информации.

В июне 2016 г. случился казус, в реестре российского программного обеспечения (ПО) были обнаружены (https://reestr.minsvyaz.ru/reestr/) экземпляры, помеченные как российские, но даже признаки принадлежности к известным иностранным продуктам выступали столь вопиюще, что правда была восстановлена (это решения «Логика ECM ASL.СЭД», «Карельская медицинская информационная система» и M1: ECM Платформа»). Просмотр реестра российского ПО сопровождался не новой мыслью, которая сопровождает авторов уже на протяжении длительного времени при анализе ландшафта индустрии информационных технологий (ИТ) в России. Авторам представляется, что никакое импортозамещение не приведет к положительным тенденциям без обретения технологического суверенитета в области ИТ. Отсутствие технологического суверенитета в области ИТ досталось России по наследству от СССР, который к моменту своего распада, утратил возможность эффективно использовать существовавшие ранее заделы по данной тематике. Под технологическим суверенитетом мы подразумеваем такое устойчивое и наблюдаемое состояние, когда реализация ИТ возможна исключительно на основе компонентов, производимых организациями в пределах юрисдикции России и имеющим на них исключительные права.

Для достижения данной цели необходимо выполнить анализ существующих требований в части касающейся. В РФ государственные регуляторы (прежде всего ФСТЭК, ФСБ) создали определенную систему (лицензирования, сертификации, аттестации), которая отражает, в значительной степени, устаревшие подходы к обеспечению ИБ. Например, документы ФСТЭК России (приказы № 21 и № 31) только упоминают необходимость учета рисков ИБ, но не предлагают полностью замкнутого цикла управления рисками ИБ – в частности, нет оценки остаточных рисков. Хотя в Приказе ФСТЭК России № 31 и упоминается стандарт ISO серии 27001 «Системы менеджмента информационной безопасности», основных «инструментов» управления (менеджмента) ИБ для «стандартных» процессов ИБ не представлено.

Документы отраслевых систем обеспечения ИБ (например, СТО Газпром СОИБ или СТО БР ИББС) также не могут демонстрировать адекватность существующих методических подходов в силу весьма ограниченного, к сожалению, представления защищаемых сущностей (объектов защиты), незамкнутой процедуры оценки (обработки) рисков ИБ или ограниченности требований к ИБ на стадиях жизненного цикла (ЖЦ) защищаемых информационных систем (ИС). Из доступных на данное время государственных стандартов в области ИБ следует с уважением отметить государственный стандарт ГОСТ РВ 0015-002-2012 «Система разработки и постановки продукции на производство военной техники. Системы менеджмента качества. Общие требования», в котором декларируется соответствие требованиям стандартов ISO серии 27001. Наблюдается логичное и обоснованное направление по включению требований по ИБ там, где это жизненно важно и критично – в области государственного оборонного заказа, т.к. требования ГОСТ РВ 0015-002-2012 там обязательны. Представляется рациональным принятие таких же требований для иных критичных отраслей экономики РФ – отрасли связи, энергетики, транспорта, добычи (транспортировки) углеводородного сырья, финансов и пр.

Соответственно, возникает вопрос существенного переосмысления всей национальной нормативной базы, т.к. в настоящий момент современный уровень ИТ и требования к обеспечению ИБ поставили «вопрос ребром» - либо переходить к национальной нормативной базе полностью основанной на современных международных стандартах (например, серии ISO/IEC 15408, ISO/IEC 27001, ISO 22301, ISO/IEC 20000, ISO/IEC 31000 и пр.), чем продолжать применять выборочно

нормативную базу российских регулирующих органов, частично «улучшенную» международными методиками (ISO, NIST, CoBIT, ILIT, COSO и пр.).

Рассмотрим, какие значимые изменения произошли в области методического обеспечения в сфере ИБ в наиболее значимых организациях в мире. В США был выпущен закон «Federal Information Security Management Act» (FISMA) во исполнение которого NIST разработал ряд нормативных документов, предусматривающих принципиально новый подход организационному обеспечению ИБ. Документы знаменитой ранее «радужной серии» утратили статус действующих. Также на международном уровне были приняты стандарты ISO/IEC 15408 «Information technology. Security techniques.Evaluation criteria for IT security» и ISO/IEC 27001 «Information technology.Security techniques. Information security management systems. Requirements». Отметим, что все указанные стандарты переведены в настоящее время и являются национальными стандартами в систем ГОСТ Р ИСО/МЭК.

«Рыночные правила игры» в области ИБ носят разнонаправленный характер, но в целом могут быть охарактеризованы по известному принципу как «доверие через оценку». Одну часть этих требований формируют различные отраслевые методики и стандарты (например, API, COBIT, Achilles, NIST, COSO), другую часть – международные стандарты (ISO, IEC, ISAGO и пр.). Необходимо сделать некоторые уточнения – современные версии многих документов в области ИБ, ранее основанных на уникальных методиках, со временем «мигрируют» на общемировые стандарты (в частности COBIT в новой версии 5 в целом соответствует ISO 38500), и также важно, что ряд важнейших стандартов ISO принимается постепенно в РФ в качестве национальных стандартов ГОСТ Р ИСО (ГОСТ Р ИСО/МЭК).

Принимая во внимание постановку задачи, важно отметить, что подход ISO 15408 «Общие критерии» по оценке соответствия также хорошо известен в РФ, равно как и его новые модификации (например, collaborative Protection Profile – совместных профилей защиты). В области оценки систем управления (менеджмента) ИБ хорошо известны стандарты ISO серии 27001, отчасти – ISO серии 20000 и серии 22301. Однако нужно признать, что количество сертификатов решений (по требованиям ISO 15408) и систем (по требованиям ISO 27001) в РФ крайне невелико по сравнению с иными странами (РФ по данным ежегодного отчета ISO 2014 г. кратно уступает Польше, Венгрии, Чехии). Этот факт можно трактовать как намерение наших ближайших европейских коллег ориентировать свои производства на западные рынки, глубоко интегрировать международные стандарты ИБ и в целом подтверждать формальное соответствие решений (услуг) через общеизвестные публичные стандарты оценки. В начале нынешнего века в блоке западных стран на разных уровнях было достигнуто понимание о необходимости отнесения вопросов ИБ к сфере компетенции ИТ. Это обусловлено как бурным развитием ИТ, в ходе которого средства обработки информации «насыщались» встроенными функциями безопасности, так что потребность в средствах безопасности вне контекста ИТ («наложенных» средствах ИБ) сошла на нет.

Рассмотрим далее возможные решения поставленной задачи импортозамещения. Прежде всего, основным риском является ориентация всех компаний-разработчиков в РФ в области ИБ на формальное соответствие требованиям государственных регуляторов, что также справедливо (но в меньшей степени) и для компаний системных интеграторов (они имеют свободу маневра при выборе различных решений в проектах ИБ). Жесткие лицензионные требования и достаточно фиксированный внутренний рынок сбыта (за редким исключением) не позволяет разработчикам в РФ предложить продукцию, выдерживающую серьезную рыночную конкуренцию, и, как следствие – не позволяет реализовать технологически суверенные решения, прошедшие оценку по международным стандартами или их национальным аналогам. В качестве рекомендации можно рассмотреть создание технологии, в которой все решения в области ИБ и их компоненты будут изначально разрабатываться в едином безопасном процессе (например: Security Development Lifecycle – SDL).

Соответственно, потребуется создать структуру, подобную CMDB (Configuration management database), как это принято в ISO 20000, ITIL и ряде других методик для контроля уровня безопасности, поддержки версионности и отслеживания «родителей» и «потомков» всех оцененных по требованиям ИБ компонент: и программных и аппаратных. Финальная «сборка» защищенных ИС возможна только из «доверенных» компонент, прошедших все положенные тесты ИБ в установленном порядке, внесенных в национальный CMDB и позволяющих обеспечивать заданный уровень ИБ адекватно поставленным требованиям. В РФ в методическом плане для реализации SDL уже существуют все необходимые национальные стандарты, в частности:

- ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Следующий риск для обеспечения требуемого уровня ИБ – создание национального полного замкнутого цикла управления ИБ, например, по образцу ЖЦ в NIST:

- Категорирование активов – FIPS 199 / SP 800-60;
- Выбор мер безопасности – FIPS 200 / SP 800-53;
- Реализация мер безопасности – SP 800-160;

- Оценка мер безопасности – SP 800-53A0;
- Мониторинг мер безопасности – SP 800-137.

Рассмотрим условия достижения технологического суверенитета в области ИТ. Важнейшим базовым условием является обладание полным спектром технологий от проектирования микроэлектронных компонентов до выпуска готовых изделий на их основе, равно как и компонент ПО, прошедших оценку доверия в уставленном порядке. Некоторые успехи в области космической и военной электроники, обеспечении органов государственной власти (ОГВ) планшетами на базе «новой гарвардской архитектуры» представляются достаточными для парирования современных вызовов в области ИБ только символически. Целесообразно привести пример пирамиды, стабильное положение которой основано на максимально широком спектре доступных доверенных компонентов ИБ и оборудования общего назначения, прошедших необходимые проверки в России.Нужно набраться мужества и честно признать, что технологический суверенитет не достижим в полной мере только на базе свободного ПО с открытым кодом, доведенного под требования ОГВ.

Следующим условием достижения технологического суверенитета в области ИТ является доверие к системе, типовым способом формирования которого в настоящее время является «доверие через оценку». Но для того чтобы получать адекватные результаты, нужно понимать в какой момент времени производить оценку. Существующая мировая практика предусматривает оценку по мере необходимости. Переложение данного подхода на наши условия диктует необходимость отказаться от лицензирования деятельности в области защиты открытой информации (оставив только безусловное обеспечение безопасности ОГВ, что следует также и из недавних разъяснений представителей ФСБ по применению «пакета Яровой») и выполнять оценку соответствия по мере необходимости в открытых и прозрачных системах оценки соответствия, поддерживаемых сообществом участников рынка ИТ. Представляется целесообразным производить оценку безопасности в ИТ в рамках ISO/IEC 15408, являющимся на сегодняшний день в мире стандартом «де-факто» и не имеющим альтернатив. В части управления безопасностью целесообразно производить оценку процессов управление в рамках ISO/IEC 27001, который в своем сегменте также является в мире стандартом «де-факто» и не имеет альтернатив.

Следующим условием достижения технологического суверенитета в области ИТ является тесная кооперация сообщества производителей компонентов ИТ между собой. Иначе достижения технологических прорывов в масштабе России не видать, т.к. пока еще слишком малы объемы и компетенции каждого производителя в отдельности, невелик их рынок сбыта и, соответственно, отраслевая экспертиза. Ранее подобная проблема называлась «комплексированием», и в работах специалистов СССР ей уделялось достойное внимание и важное место в процессе создания надежных решений ИТ из различных компонент

Следующим условием является обеспечение компетентных кадров для создания безопасного ЖЦ решений в области ИБ. К сожалению, необходимо констатировать невысокий общий уровень специалистов, заканчивающих профильные специальности по ИБ даже в ведущих ВУЗах РФ. По итогам участия в аттестации магистров и бакалавров приходится констатировать следующее «расслоение» - выпускные работы либо делаются полностью под требования государственных регуляторов (например, по защите персональных данных), при этом абсолютно не принимаются в расчет существующие в мире стандарты; либо разрабатываются решения полностью под зарубежные спецификации, не принимая во внимание, например, национальные ограничения в области криптографии).

Вывод. Заявленные в представленной публикации цели могут показаться амбициозными и загоризонтными. Но если не ставить таких целей на уровне отраслей в России, а просто «плыть по течению» только на волнах свободного ПО с открытым кодом, то и через много лет мы опять окажемся, к сожалению, на том же самом месте – в самом начале тяжелого и длинного пути к национальному технологическому суверенитету.

Лопатин Д.В., Анурьева М.С., Остапчук К.И., Ерёмина Е.А., Пузанова Я.М., Житенева И. А.
Россия, г. Тамбов, Тамбовский государственный университет имени Г.Р. Державина

ПРОБЛЕМА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ УГРОЗ В РЕГИОНЕ

Официально в МВД России преступления в области информационных технологий относятся к группе преступлений в сфере телекоммуникаций и компьютерной информации. Согласно открытым данным отдела «К» УМВД РФ по Тамбовской области, характерными правонарушениями являются: взломы компьютерных систем, кражи паролей для доступа в сеть Интернет, распространение вредоносных программ и т. п.; неправомерный доступ к компьютерной информации; нарушение тайны переписки, телефонных переговоров; мошенничество в интернете; незаконный оборот средств шпионажа; распространение детской порнографии; создание фишинговых ресурсов и сайтов, специализирующихся на клевете и компрометирующих материалах. Рассмотрим наиболее яркие преступления в ИТ сфере за последнее время. Имеются случаи неправомерного доступа к компьютерной информации. В регионе отмечены случаи взлома сайтов государственных структур.

Участились случаи шантажа пользователей информацией личного характера с целью вымогательства. Особенно частыми оказались мошеннические схемы хищения денежных средств с банковских карт путем размещения объявлений о купле-продаже в сети Интернет. Зарегистрированы случаи неправомерного доступа к банковской карте посредством социальной инженерии.

Отношение пользователей к проблеме инфокоммуникационных угроз

Действенным методом исследования является применение традиционных методик анкетирования различных возрастных групп, что позволяет получить детальную первичную информацию об актуальном уровне ИКТ-угроз для пользователя, его восприятии проблемы, уровне знаний о методах и средствах блокирования деструктивных информационных воздействий. Разработаны оригинальные анкеты для различных возрастных групп, позволяющие получить первичную информацию об актуальном уровне ИКТ-угроз для пользователей. Разработанный метод обработки анкет в реальном времени позволяет получать статистические выборки по группам респондентов для анализа полученной информации.

Разделим всех пользователей на две группы. Первая – это пользователи, имеющие профессиональное отношение к ИКТ (программисты, инженеры технической поддержки и продвижения проектов компаний по разработке программного обеспечения). Вторая группа – простые пользователи ИКТ (военнослужащие, бухгалтеры, дизайнеры интерьеров, домохозяйки, мастера производства, медсестры и др.).

Анализ результатов анкетирования показал, что пользователи и первой, и второй группы менее всего информированы о вирусных угрозах. Почти все опрошенные пользователи обоих групп (~70 %) обладают начальными знаниями об вирусных угрозах. 27% респондентов первой группы и 11% респондентов второй группы имеют средний уровень знаний.

В силу своей профессиональной деятельности половина респондентов первой группы (специалисты в определенной области ИКТ) показывают хорошие знания информационных угроз, связанных с манипулированием действиями пользователя в сети. Другая половина пользователей этой же группы имеет только средний уровень знаний об угрозе. Чуть больше половины опрошенных респондентов второй группы обладают средними знаниями об угрозе манипулирования сознанием и действиями пользователя. Только четверть опрошенных пользователей второй группы хорошо понимают данную угрозу. У 16% пользователей этой же группы есть только начальные знания о данной угрозе.

Анализ материалов по анкетированию показал, что уровень знаний об угрозах, связанных с мошенничеством в сети и фишингом, у респондентов первой группы значительно выше, чем у второй группы. Так около 10% пользователей первой группы имеют профессиональное понимание данных угроз. 45% респондентов из первой группы имеют хорошие знания. В тоже время, примерно половина пользователей этой же группы имеют только средний или начальный уровень знаний. У второй группы только 10 % респондентов хорошо понимают угрозы связанные с фишингом. 46% и 41% пользователей имеют средний или начальный уровень знаний о данной угрозе, соответственно.

Рассмотрено отношение респондентов к основным угрозам инфокоммуникационного характера (вирусные атаки, интернет-фишинг и манипулирование сознанием и действиями в сети). Из результатов исследования видно, что опасным рискам в области вирусных атак подвержены все рассмотренные группы пользователей. 70% пользователей первой и 78% пользователей второй группы имеют только начальные знания об угрозе. Несколько иначе обстоит ситуация в области манипулирования чуть больше половины опрошенных респондентов второй группы обладают средними знаниями о данной угрозе. Меньший уровень угроз для респондентов первой группы может объясняться наличием профессиональных компетенций в области ИКТ и опытом работы. Однако, примерно половина пользователей этой группы в целом показывают только средний и начальный уровень знаний. Необходимо уделить внимание развитию навыков практической безопасности в первую очередь для блокирования вирусных угроз и мошенничеству в сети.

Макаров А.С., Москвин Д.А. Иванов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

РАЗРАБОТКА ЗАЩИЩЁННОГО USB НАКОПИТЕЛЯ

На сегодняшний день одним из самых популярных средств передачи и хранения информации по-прежнему остаются USB-накопители. Основными преимуществами данного средства хранения и передачи информации являются: срок хранения информации, энергонезависимость используемой памяти, устойчивость к механическим повреждениям, компактность и многое другое. Более того классические USB-накопители позволяют пользователям хранить и передавать информацию без участия третьей стороны, которой, например, может являться владелец облачного хранилища.

Несмотря на перечисленные достоинства, USB-накопители имеют ряд недостатков. Конфиденциальная информация, записанная на накопителе, никак не защищена, поэтому завладев устройством, злоумышленник получает доступ к конфиденциальным данным или может осуществить запись вредоносного программного обеспечения в память устройства.

Таким образом, в настоящее время актуальной становится задача разработки подходов к обеспечению защиты информации, хранимой и передаваемой с помощью USB-накопителей, от несанкционированного доступа. На данный момент практически все существующие USB-накопители имеют существенные недостатки, которые проявляются в неудобстве эксплуатации, низкой степени надёжности и необходимости сложных манипуляций, связанных с настройкой и наладкой корректной работы накопителя.

Для разработки нового подхода и опытного образца было решено три задачи:

- исследование существующих подходов к обеспечению защиты информации, хранящейся на USB-накопителе;
- формирование концепции для подхода, основанного на сравнении достоинств и недостатков существующих решений;
- разработка экспериментального образца.

Исследовав существующие подходы, были выявлены их достоинства и недостатки. Наилучшим подходом к обеспечению безопасности является аппаратное шифрование данных самим накопителем. Немаловажным моментом является возможность смены ключа шифрования данных и отдельного надёжного его хранения. А добавление возможности защиты устройства от записи позволит избежать нарушения целостности конфиденциальной информации при работе за недоверенным ПК.

Таким образом новый подход заключается в обеспечении защиты информации с помощью криптостойкого алгоритма шифрования, ключ для работы которого, будет храниться в защищённых областях памяти в смарт карте. Ключ шифрования должен быть разделён на две части и помещён в разные защищённые части памяти смарт карты. Разделение ключа шифрования на две половины и расположение разных частей в разных защищённых блоках памяти позволяет повысить надёжность хранения ключа шифрования, так как для доступа к нему необходимо пройти аутентификацию уже к двум блокам памяти защищенной смарт-карты. Хранение прав доступа также происходит в защищённой области смарт карты.

Для разработки эксперементального образца необходимо выбрать элементную базу. В качестве памяти было принято решение использовать microSD карты, так как это надёжный и дешёвый компонент. Для хранения ключа шифрования была выбрана бесконтактной смарт карта фирмы, имеющая беспроводной интерфейс. Такое решение не будет сопровождаться износом элементов под физическим воздействием и будет удобно для использования. В качестве микроконтроллера был выбран продукт, обладающий высоким быстродействием, наличием необходимых интерфейсов и аппаратным шифрованием криптостойким алгоритмом шифрования.

Предложенный подход к защите информации был реализован в экспериментальном образце, который совмещает в себе достоинства разных реализаций в одном устройстве, а также дополняет функционал системой контроля доступа, которая позволяет ограничить некоторым пользователям возможность записи или модификации информации. Предложенный подход позволяет обезопасить конфиденциальные данные от злоумышленника при условии раздельного хранения смарт карты от накопителя.

Малов С.С., Юмашева Е.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Во многих организациях используют систему контроля управления доступом (СКУД). Основной задачей СКУД является управление доступом на заданную территорию через некие точки доступа, а также идентификация лица, имеющего доступ на заданную территорию.

Соответственно, в СКУД хранится информация обо всех сотрудниках, которые имеют право прохода на территорию организации, а также посетителях получивших временный пропуск. К этой информации относятся сведения о ФИО, паспортные данные, а иногда и фотография.

Данный набор сведений, согласно Федеральному закону от 27.07.2006г. №152-ФЗ «О персональных данных, относится к персональным данным (ПДн) и, следовательно, должен быть защищен, а СКУД является информационной системой персональных данных (ИСПДн).

При обеспечении защиты ИСПДн необходимо руководствоваться положениями Постановления Правительства РФ от 01.11.2012г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Оно определяет, что перед проектированием системы защиты необходимо используя результаты предпроектного обследования определить уровень защищенности ИСПДн, который определяется по четырем критериям:

1. Тип угроз, актуальных для ИСПДн;
2. Субъект ПДн (сотрудник или не сотрудник организации);
3. Объем обрабатываемых ПДн;
4. Категория обрабатываемых ПДн.

При определении категории ПДн, обрабатываемых в ИСПДн, необходимо руководствоваться нормативно-правовыми актами Российской Федерации. Согласно нормативным документам ПДн могут быть отнесены к одной из следующих категорий:

1. специальные;
2. биометрические;
3. общедоступные;
4. иные.

При определении категории ПДн, обрабатываемых в СКУД, сложность возникает с определением необходимости считать ли фотографию биометрическими ПДн, т.к. известно, что к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Это могут быть физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись).

Как уже было отмечено, в СКУД идентификация человека происходит путем сравнения фото на пропуске с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД. Таким образом имеет место быть совокупность использования персональных данных человека. К сожалению, нормативно-правовая база Российской Федерации не дает однозначного ответа на вопрос, является ли фотография в СКУД биометрическими персональными данными. Что приводило к спорам и субъективным подходам при определении категории ПДн, обрабатываемых в СКУД.

Точку в данном вопросе поставила организация, выступающая в роли регулятора в области защиты персональных данных, - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 30.08.2013г. Роскомнадзор. выпустил "Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки", в которых указал, что «фотографическими изображениями сотрудников организации, содержащимися в системе контроля управления доступа (СКУД), являются биометрическими персональными данными, поскольку характеризуют физиологические и биологические особенности человека, позволяющие установить, принадлежит ли данному лицу предъявляемый СКУД пропуск, на основе которых можно установить его личность путем сравнения фото с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД».

Таким образом при определении уровня защищенности СКУД, в которой обрабатываются ПДН, нужно учитывать что категория ПДн будет биометрической, а это накладывает дополнительные требования при организации защиты ИСПДн.

Малышев Е.В., Павленко Е.Ю., Зегжда П.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ВЫЯВЛЕНИЕ АВТОМАТИЧЕСКИ УПРАВЛЯЕМЫХ УЧЕТНЫХ ЗАПИСЕЙ В СОЦИАЛЬНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

В соответствии со статистическими данными, более 30% населения планеты являются активными пользователями социальных сетей. Использование социальных сетей позволяет пользователям общаться, знакомиться, а также получать актуальную информацию и новости. Люди регулярно заходят в социальные сети с целью получения информации о социальной, политической и экономической обстановке в стране и мире. На сегодняшний день одним из самых популярных методов общения социально и политически активных слоев населения являются социальные сети, при этом они предоставляют не только средства общения, но и возможность активного выражения своей позиции и обсуждения наиболее острых вопросов.

Большинство пользователей указывают на своей странице достоверную информацию о себе, такую как имя, фамилию, год рождения, город проживания, возраст, сферы увлечений и т.п. Помимо этого, пользователи объединяются в группы на основе общих интересов и увлечений. С помощью данной информации становятся возможными группирование и классификация пользователей по различным признакам. В тематических группах, в свою очередь, публикуются новости и записи, просматриваемые большинством участников, в результате у пользователя, просматривающего последние новости, на их основе формируется мнение о сложившейся обстановке в стране и мире.

Для злоумышленников возможность разбиения пользователей социальной сети на группы по различным признакам является важным фактором, позволяющим воздействовать на мнение пользователей и на формирование общественной позиции. В настоящее время социальные сети являются инструментом для формирования общественного мнения, в том числе, для стимулирования пользователей на совершение различных нелегитимных действий. Однако для сильного воздействия

на общество необходима массовость продвигаемой идеи: большое число постов, комментариев, создание соответствующих сообществ. Для этого используются автоматически управляемые аккаунты (боты), которые контролируются лицами, заинтересованными в продвижении своих идей в широкие массы. Злоумышленники имеют возможность создания крупномасштабных, в основном состоящих из ботов, сообществ, характеризующихся определенным социальным настроем и влияющих на формирование определенной гражданской позиции у пользователей. Существующие методы противодействия ботам в социальных сетях недостаточно эффективны, так как они основываются на детектировании ботов при помощи модераторов, борьба с автоматизацией процессов происходит при помощи CAPTCHA. Поэтому в настоящий момент блокировка ботов возможна только после проявления их активности, при этом модераторы физически не смогут проверить все подозреваемые аккаунты.

В работе предлагается использовать методы машинного обучения для решения описанной проблемы распознавания автоматически управляемых аккаунтов, в частности, нейронные сети, поскольку они хорошо себя зарекомендовали в решении задач распознавания образов. Для распознавания образов предлагается применять персептрон, использующий метод обратного распространения ошибки. Метод обратного распространения ошибки – метод обучения многослойного персептрона, основная идея которого заключается в распространении сигналов ошибки от выходов сети к ее входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы. Алгоритм обратного распространения ошибки является одним из методов обучения многослойных нейронных сетей прямого распространения, называемых также многослойными персептронами. Многослойные персептроны успешно применяются для решения многих сложных задач, в том числе задач распознавания образов.

Для обучения разработанной нейронной сети была сформирована обучающая выборка пользователей социальной сети «ВКонтакте», на ее основе выполнена настройка весов сети. Для успешного обучения необходимы вектора, описывающие страницы и ботов, и реальных пользователей. Для получения выборки реальных пользователей были использованы верифицированные страницы. Для получения выборки заблокированных пользователей была сохранена информация о 100 000 последних зарегистрированных пользователях. Через неделю информация о аккаунтах была получена повторно, из них 26 500 было заблокировано. Полученная выборка была использована для обучения в качестве ботов, на ее основе произведена настройка весов нейронной сети для распознавания ботов в социальных сетях с наибольшей вероятностью.

Предлагаемый подход к обнаружению автоматически управляемых аккаунтов в социальных сетях на основе нейронных сетей является эффективным средством выявления ботов. Он может быть использован для проверки как сообществ, так и пользователей социальной сети на наличие в них ботов, что позволяет предотвращать попытки влияния на гражданскую позицию у пользователей социальной сети.

Марков В.С., Сидоренко Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский научный центр Российской академии наук

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Применение технологий облачных вычислений определяет необходимость рассмотрения возможных способов дестабилизирующих воздействий, приводящих к нарушению функционирования компонентов информационной среды.

Особую опасность предоставляют угрозы, которые реализуются внутри периметра безопасности компьютерной сети, так как их локализация с применением современных средств защиты информации, например, антивирусов и сканеров безопасности, встречает существенные трудности. Атаке могут подвергнуться как элементы сетевой инфраструктуры провайдера, который предоставляет облачные услуги, так и сама среда виртуализации.

Если традиционные средства защиты работают на уровне операционных систем и аппаратной части ИТ-среды, то важнейший компонент облака — средства виртуализации — расположен между ними и тоже требует защиты, в том числе от администраторов виртуальной инфраструктуры, от перегрузки аппаратных ресурсов, от некорректного обращения с данными разных клиентов при их совместном хранении. Вследствие особенностей архитектуры самих виртуальных сред трафик между серверами, расположенными в пределах одного хостового физического сервера, замкнут на уровне гипервизора. Таким образом, применение традиционных систем защиты информации в виртуальной среде становится не эффективным. Возникает угроза реализации бесконтрольных атак из скомпрометированной виртуальной машины на соседние машины. Более того не все аппаратные средства защиты будут работать в виртуальной среде. Например, аппаратные межсетевые экраны не могут разграничить доступ к различным серверам, находящимся внутри одного хоста. Они не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, а сам сетевой трафик не покидает серверы виртуализации

и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование. Кроме того, виртуальные машины одного физического сервера могут обмениваться трафиком напрямую, без участия физических сетевых коммутаторов. Таким образом, использование физических межсетевых экранов не будет эффективным.

В работе рассматривается один из подходов обеспечения информационной безопасности облачных технологий, обеспечивает динамическое управление сетью вне зависимости от физического расположения виртуальных ресурсов.

Меркушев Е.С., Котенко И.В.
Россия, Санкт-Петербург, Санкт Санкт-Петербургский институт информатики и автоматизации Российской академии наук,

АНАЛИЗ СВОЙСТВ ЭКОСИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Облачные вычисления становятся успешной и популярной бизнес-моделью из-за их привлекательных особенностей. В дополнение к очевидным преимуществам, эти особенности также влекут за собой характерные облакам серьезные проблемы безопасности. Проблемы безопасности стали доминирующей преградой перед разработкой и широким использованием облачных вычислений. В докладе экосистема облачной безопасности анализируется с точки зрения пяти различных свойств: конфиденциальности, целостности, доступности, подотчетности и приватности. Эти свойства являются наиболее состоятельными в современных научных исследованиях.

Среди облачных уязвимостей особое внимание уделяется следующим: сосуществование виртуальных машин (ВМ), потеря (пользовательского) физического контроля над данными, пропускная способность при инициализации и облачная модель ценообразования.

Пользователи хранят свои данные и вычислительные задачи на облачных серверах, которые контролируются потенциально ненадежными провайдерами. Среди угроз облачной конфиденциальности следует выделить следующие: кросс-ВМ атаки по скрытым каналам (выемка данных при этой угрозе может производиться посредством измерения использования кэша, оценки объема трафика, атаки по времени для нажатия клавиш), вредоносный системный администратор (привилегированный сисадмин может осуществлять атаки с помощью доступа к данным пользовательских ВМ). Характерные для облаков подходы к решению проблем кросс-ВМ атак делятся на две категории: предотвращение сосуществования и соблюдение физической изоляции.

Понятие целостности в облачных системах включает в себя как целостность данных, так и целостность процессов обработки данных. Относительно этого атрибута, критическое значение имеют такие угрозы, как потеря/изменение данных, некорректные вычисления на удаленных серверах. Для проверки целостности данных разработаны различные методы «доказуемого» хранения данных (PDP) и метод «доказательства возможности возвращения» данных (POR). К актуальным требованиям проверки целостности данных относится возможность динамического изменения файлов и их распределенного хранения. Что касается целостности вычислений, то на сегодняшний момент используется реплицирование вычислений, удаленная аттестация (оборудование генерирует для клиента сертификат, содержащий информацию о программном обеспечении (ПО)), ведение подробных журналов вычислительных операций.

Доступность имеет определяющее значение, поскольку основной функцией облачных вычислений является предоставление по запросу пользователя услуг различных уровней. Угрозы доступности облака можно разделить на атаки типа «отказ в обслуживании» и атаки мошеннического потребления ресурсов. От новых типов DoS-атак частично защититься позволяет миграция сервиса. Для обнаружения EDoS-атак используются различные алгоритмы сравнения текущего трафика со статистическими данными.

Подотчетность и ответственность сторон была хорошо изучена в других системах, однако и в сфере облачных технологий она является фундаментом доверительных отношений клиента и провайдера. Можно выделить ряд угроз, касающихся облачной ответственности: нарушение соглашения о предоставляемых услугах (причиной могут стать неправильные настройки серверов, недостаточное количество выделенных пользователю ресурсов, наличие внедренного вредоносного кода в клиентском ПО, недоступность данных), недобросовестное использование MapReduce (можно рассматривать как проблему вычислительной целостности), скрытая идентификация злоумышленников, нечеткое определение потребляемых ресурсов. Для защиты предлагается вести подробные журналы операций, использовать выборку образцов для вероятностного подтверждения, ответственные виртуальные машины (AVM), совместный мониторинг.

Приватность пользовательских данных – в настоящее время это вопрос высшего приоритета. Некоторые свойства безопасности прямо или косвенно влияют на сохранение секретности: целостность гарантирует, что данные не повреждены; подотчетность, наоборот, может подорвать приватность из-за того, что способы достижения этих двух свойств безопасности обычно

конфликтуют. В некоторых случаях сохранение приватности является более жесткой формой конфиденциальности, ввиду того, что оба аспекта связаны с предотвращением утечки информации.

В настоящем докладе проводится систематизация проблем безопасности, касающихся облачных вычислений: определяются наиболее значимые свойства (конфиденциальность, целостность, доступность, подотчетность и приватность), выделяются угрозы и соответствующие им уязвимости, а также обсуждаются стратегии защиты.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Минин А.А., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

УГРОЗЫ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ДИНАМИЧЕСКИХ СЕТЕЙ VANET/MANET

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

Мобильная динамическая одноранговая сеть MANET и, ее разновидность транспортные сети VANET – сети, в которых узлы могут выполнять функции клиента и маршрутизатора, а также применяются одноранговые протоколы маршрутизации. Такого рода сети активно используются в интернете вещей, сенсорных сетях, транспортных сетях для организации связи между перемещающимися узлами и при построении умных (smart) сетей различного уровня сложности. В такого рода сетях устройство может постоянно менять свое местоположение, но все посланные ему сетевые пакеты должны быть доставлены. В дополнение к угрозам кибербезопасности, характерным для классических проводных и беспроводных сетей, одноранговые сети обладают специфическим набором угроз конфиденциальности, целостности и доступности.

Минин А.А., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

МЕТОД ЗАЩИТЫ ОТ УГРОЗ ДОСТУПНОСТИ СЕТЕЙ ТИПА M2M ПУТЕМ ДИНАМИЧЕСКОЙ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

Масштабное распространение устройств, поддерживающих межмашинное взаимодействие, а также технологий M2M в мобильных сетях MANET и сетях транспортных средств VANET, привело к тому, что классические способы построения компьютерных сетей стали малоэффективными ввиду огромного числа узлов, которые постоянно меняют свое местоположение. В таких сетях применяются технологии организации прямого взаимодействия между устройствами и алгоритмы одноранговой маршрутизации, в которых устройства одновременно выполняют функции клиента и маршрутизатора.

Маршрутизация в одноранговых сетях основана на метриках соединений, что приводит к тому, что, имитируя лучшую метрику, узел-нарушитель может переориентировать сетевые потоки. Существует два подхода к реализации маршрутизации в одноранговой сети – проактивный и реактивный. При проактивном подходе все устройства сети знают всю топологию сети и могут построить путь до любого другого узла. Такой подход неэффективен для крупных сетей. При реактивном подходе маршрут строится перед отправкой данных, и в большой одноранговой сети данный процесс может занять продолжительное время. Таким образом, обеспечение безопасности динамической одноранговой сети является вычислительно сложной задачей.

Для реализации возможности применять средства защиты в такой сети необходимо большую сеть разбить на несколько подсетей, и на устройствах, соединяющих разные подсети, организовать фильтрацию трафика.

Для разбиения на подсети предлагается использовать муравьиный алгоритм: весь распространяемый по сети трафик помечается феромоном, при проходе через любое устройство феромон откладывается на нем. Устройства, преодолевшие определенный уровень феромона, становятся кандидатами на то, чтобы стать граничными узлами. Для этого они должны поддерживать фильтрацию трафика и пройти регистрацию в центре безопасности. Общение между устройствами из разных областей возможно только через граничные узлы. Подход позволяет создать фильтрацию трафика между различными сегментами, но если устройства взаимодействуют в рамках одного сегмента, то трафик не фильтруется. Для фильтрации внутри сегмента необходимо выбрать внутренний узел фильтрации. Выбор такого устройства происходит аналогично выбору граничного

узла. Если ни одно из устройств не подходит по критериям выбора, то внутренним устройством фильтрации назначается граничный узел (рисунок). При построении маршрута от узла-источника до узла назначения в рамках одной области, накладывается ограничение, что трафик должен пройти через узел фильтрации трафика, а такое ограничение реализуется как при использовании проактивного, так и при использовании реактивного подхода к маршрутизации.

Предложенный подход позволяет строить большие одноранговые M2M-сети с фильтрацией трафика и поддержкой функций контроля доступа. Описанный подход позволяет локализовать воздействия атак типа "черная дыра" и "воронка" в рамках одной подсети, атаки типа "червоточина" становится нереализуемой.

Михайлов М.В., Чечулин А.А.
Россия, г. Ярославль, Ярославский государственный университет им. П.Г. Демидова,
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации
Российской академии наук

КЛАСТЕРИЗАЦИОННО-КОРРЕЛЯЦИОННЫЙ СКАНЕР ХРАНИЛИЩА ДАННЫХ

Методики интеллектуального анализа данных неразрывно связаны со сбором статистических данных об исследуемом процессе. Эмпирико-статистическая информация собирается в хранилище данных, откуда в последующем выбирается для анализа и выявления связанных фактов. Особого внимания при этому заслуживают методы анализа временных рядов.

Временные ряды из хранилища данных можно получить путём выборки фактов по времени. В настоящей работе предлагается проводить анализ полученных временных рядов с помощью кластеризационно-корреляционного сканера.

Кластеризационно-корреляционный сканер – это процедура, которая группирует объекты (в рассматриваемом случае временные ряды) таким образом, что в каждом кластере оказываются временные ряды близкие друг другу по определённой мере близости.

Мера близости для временных рядов заслуживает особого рассмотрения, поскольку классические расстояния (эвклидово расстояние, расстояние по Хеммингу, расстояние Чебышева, расстояние Махаланобиса, пиковое расстояние) не подходят для временных рядов. Искомую меру близости можно построить на коэффициенте корреляции или вейвлет коэффициентах. При сравнении этих мер близости для кластеризационно-корреляционного сканера можно выявить следующие факты:

1. мера близости на коэффициенте корреляции учитывает только линейные связи между временными рядами, в то время как мера близости на вейвлет коэффициентах учитывает и нелинейные зависимости;
2. при кластеризации по мере близости основанной на коэффициенте корреляции можно построить регрессионную модель для каждого кластера, при этом учитывая связи с запаздыванием по времени относительно друг друга;
3. при кластеризации по мере близости на вейвлет коэффициентах, чтобы найти нелинейные связи с запаздыванием относительно друга, нужно повторять процедуру вычисления близости каждый раз, сдвигая 1 из 2 сравниваемых временных ряда на дискретный шаг времени факта (секунда, минута, час, сутки, неделя и так далее).

Алгоритм кластеризации по мере близости основанной на коэффициенте корреляции можно представить следующим образом:

1. делим множество временных рядов на два блока методом деления пополам;
2. выделяем случайным образом (или неслучайным) один временной ряд из любого из 2-х блоков;
3. считаем множественный коэффициент корреляции к каждому из двух блоков и полученному ряду из блока шага 2;
4. выбираем группу с наибольшем коэффициентом множественной корреляции и передаём группу на шаг 1;
5. продолжаем шаги 1-4 до тех пор пока группа временных рядов не выродится 1-2 временных ряда;
6. если на последнем шаге остаётся 2 временных ряда , то по каждому из них вычисляем коэффициент корреляции с временным рядом полученным на шаге 2 и выбираем 1 из 2 временных рядов с наибольшим значением коэффициента корреляции и добавляем его в кластер;
7. если на последнем шаге остаётся 1 временной, то просто добавляем его в кластер;
8. продолжаем алгоритм до тех пор, пока коэффициент корреляции не будет по модулю меньше, чем заранее заданное значение.

В дальнейшей работе предполагается развитие данного алгоритма для повышения скорости работы и снижения ресурсоемкости.

Работа выполнена при финансовой поддержке РФФИ (проект №16-37-50067).

Москвин Д.А., Мясников А.В.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

СИНХРОНИЗАЦИЯ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ ПО БЕЗОПАСНОМУ КАНАЛУ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ NFC

Поддержание пользовательских данных в актуальном состоянии и возможность доступа к этим данным с любого устройства – основополагающий принцип обеспечения удобства взаимодействия пользователя с информационными системами. Как правило, синхронизация пользовательских данных выполняется с использованием промежуточных информационных каналов. Пользовательские данные загружаются и хранятся в облачных средах, откуда посредствам интернета скачиваются на целевое устройство. В этом случае ответственность за безопасность хранения и доставки данных возлагается на поставщика инфраструктуры облачных услуг.

Однако, если безопасность пользовательских данных не может быть доверена облачным сервисам, или, если используемые устройства не имеют доступа к таким сервисам, необходим альтернативный безопасный и надежный канал синхронизации. В качестве такого канала авторами предлагается использование технологии NFC, а в качестве промежуточного носителя данных – мобильный телефон.

Технология NFC, позволяет передавать данные на расстоянии до 10 см посредством радиосигнала. Современные мобильные телефоны на базе ОС Android поддерживают технологию Host Card Emulation, которая позволяет запрограммировать свой сервис-обработчик для входящих NFC-команд, при этом на уровне ОС гарантируется, что данные, полученные от NFC-контроллера, поступят исключительно в заданное приложение. Практическая скорость работы NFC (около 400 кбит/с) не позволяет передавать большие объемы данных, поэтому данный канал связи можно использовать для первичного обмена ключами с целью установления альтернативного шифрованного канала для непосредственной передачи основного массива данных. В качестве альтернативного канала, например, могут быть использованы Bluetooth-соединение, wi-fi peer-to-peer и др.

Технология NFC хорошо подходит для установления шифрованного канала, т.к. защищает от широкого спектра атак, направленных на перехват или модификацию данных, передаваемых по беспроводному каналу. В частности, данная технология устойчива к атакам:

- пассивной прослушки, путём установления защищенного соединения с использованием протоколов ассиметричной криптографии;
- повреждения данных, путём введения контроля целостности, также данные атаки обнаруживаются приёмопередатчиками и могут быть успешно детектированы;
- модификации данных, путём использования приптографии;
- вставки данных, путём использования криптографии;
- типа Relay, путём экранирования передающего устройства, а так же использования ввода пользователя при проведении операций передачи данных
- типа «человек посередине» на уровне физической организации протокола. Данная атака невозможна ни в одной из возможных конфигураций

Встроенное API ОС Android позволяет создать защищенное хранилище, доступ к которому будет иметь только строго определенное приложение, а данные в нём будут зашифрованы и расшифровка будет происходить только при введение корректного кода. Таким образом средствами ОС можно обеспечить надёжное место для хранение синхронизируемых данных.

Кроме того, использование технологии NFC позволяет использовать мобильный телефон в качестве ключа и отслеживать, находится ли он в поле действия NFC-считывателя. Как только телефон убирается, можно производить очистку синхронизованного профиля с компьютера. Таким образом решается проблема временного развертывания пользовательского профиля, включая логины, пароли, настройки браузера и пр., на рабочей станции.

Москвин Д.А., Дахнович А.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

СХЕМА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ МЕЖДУ КЛИЕНТАМИ И ТОЧКАМИ ДОСТУПА Wi-Fi

Беспроводные технологии становятся наиболее распространенным средством коммуникации между цифровыми устройствами, и, в частности, технология Wi-Fi становится с каждым годом все более распространенным средством подключения к сети Интернет. По статистике компании Cisco, в 2014 году на беспроводные сети приходилось 46% всего мирового сетевого трафика, а к 2019 по их прогнозу эта цифра может увеличиться до 66%. Несмотря на очевидный рост популярности Wi-Fi сетей и точек доступа Wi-Fi, существует ряд атак, позволяющих скомпрометировать данные пользователя.

Одной из самых опасных атак являются атака поддельной точки доступа (англ. rogue access point). Атака заключается в следующем: злоумышленник на основе SSID (Service-Set Identifier, иначе говоря, имя сети) сетей Wi-Fi, к которым когда-либо подключался клиент, либо на основе имен

распространенных сетей, как правило, открытых, настраивает точку доступа с данным SSID, заставляя устройство пользователя подключиться именно к ней, например, физически перемещая свой точку ближе к клиенту, либо заглушая сигнал точек данной сети, к которым потенциально клиент может подключиться или уже подключен. В любом случае злоумышленник должен сделать так, чтобы сигнал от поддельной точки доступа стал сильнее, нежели от оригинальной. Таким образом, если устройство клиента успешно подключилось к подобной поддельной точек доступа, злоумышленник получает полный контроль над его данными, передаваемыми в сеть.

Данная атака возможна по нескольким причинам. Первая причина заключается в том, что не все сети предусматривают взаимную аутентификацию. Например, открытые сети. И если пользователь когда-либо подключался к открытым публичным сетям, то его устройство уже уязвимо к атаке поддельной точки доступа. Стоит отметить, чтое корпоративные сети, защищенные по протоколу WPA2 Enterprise, обычно настраиваются для аутентификации клиентов в сети, но не точек доступа клиентами. Кроме того, в Wi-Fi сети идеологически заложены следующие технологии: роуминг и идентификатор SSID. Роуминг – это процесс переассоциации клиента с другой точкой доступа, чтобы клиент мог перемещаться в пространстве без потери соединения с сетью. Идентификатор SSID позволяет точкам обозначать некоторую сеть. Так как сеть может обслуживаться несколькими точками, то SSID не уникален для каждой из них, поэтому любая точка, которая настроена с таким же SSID, будет автоматически принадлежать данной сети.

На основе вышеизложенного авторами предлагается ввести дополнительную схему аутентификации, которая бы поддерживала как одностороннюю аутентификацию точек доступа клиентами, так и взаимную аутентификацию между клиентами и точками доступа. Далее будем рассматривать одностороннюю схему. Для того, чтобы аутентифицировать точку доступа сети, необходимо ввести в дополнение к SSID некий параметр. Таким параметром предлагается использовать пару ключей, случайно сгенерированных на точке доступа, а для аутентификации использовать схему электронно-цифровой подписи на основе эллиптических кривых, так как именно протоколы ЭЦП на основе эллиптических кривых позволяют при малых размерах ключей обеспечивать тот же уровень криптостойкости, что и ЭЦП на основе чисел. Схема односторонней аутентификации выглядит следующим образом:

1. Клиент подключается к точке доступа, которую он считает доверенной (например, точке доступа, обеспечивающую домашнюю сеть).
2. Клиент получает открытый ключ данной точки доступа и запоминает его, ассоциируя данный ключ с MAC-адресом точки.
3. При последующем подключении до того, как клиент начнет передавать трафик к ТД, сначала производится ее аутентификация:
   - Клиент посылает некоторую случайную последовательность байтов точке доступа.
   - Точка подписывает данную последовательность байт на своем закрытом ключе и отправляет результат подписи клиенту.
   - Клиент проверяет полученную подпись с помощью ОК ТД и удостоверяется, что ТД обладает верным ЗК.
4. При успешной аутентификации ТД клиент начинает передачу трафика к ней, иначе подключение отменяется.

Практически данную схему можно реализовать одним из нескольких способов:

1. На канальном уровне в пакетах аутентификации протокола 802.11. Данные пакеты изначально предназначались для аутентификации и имеют все необходимые для этого поля. Однако, реализация данным способом является более затратной.
2. На транспортном уровне по средствам TCP-сокетов.
3. На прикладном уровне по средствам HTTP-сокетов.

Последние два способа идеологически не различаются и работают уже после того, как клиент подключился к точке. Поэтому клиенту необходимо блокировать исходящий трафик до того, как он аутентифицировал точку доступа. Данный способ является менее затратным для реализации.

Никитин А.С., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ПРОТИВОДЕЙСТВИЕ АТАКАМ ДЕАНОНИМИЗАЦИИ В АНОНИМНОЙ СЕТИ TOR НА ОСНОВЕ СТАТИСТИЧЕСКИХ ИССЛЕДОВАНИЙ

Проблема безопасной передачи информации через интернет может заключаться не только в обеспечении конфиденциальности самой информации, но и в необходимости обеспечить анонимность сторон, участвующих в передаче. Одним из решений является использование анонимной сети TOR, представляющей из себя систему прокси-серверов, с использованием которых возможно установление сетевого соединения с целевым ресурсом, защищенного не только от прослушивания, но и предоставляющего достаточный во многих случаях уровень анонимности. Такие свойства достигаются за счет использования луковой маршрутизации, скрывающей от

промежуточных узлов, участвующих в передаче сообщения, его настоящий источник и пункт назначения. Еще одной особенностью сети TOR является малая задержка передачи данных, что необходимо для использования интерактивных сетевых протоколов поверх сети.

Существует ряд атак на сеть TOR, использующих особенности реализации и функционирования сети, и ставящих своей целью деанонимизацию пользователей. Наиболее известными являются атаки пересечения и подтверждения. Атаки пересечения – целый класс атак, основывающийся на возможности снятия трафика на точках входа и выхода анонимной сети и сравнения статистических параметров трафика для соотнесения пользователей и ресурсов, к которым те обращаются. К таким параметрам относится время прохождения пакетов, их число, размер, и т.д.

Если атакующий имеет возможность снимать трафик конкретного пользователя, ему не требуется доступ к трафику всех выходных узлов. После предварительного проведения атаки Сибиллы, в ходе которой в сеть вводится некоторое число подконтрольных узлов, пользователь с определенной вероятностью будет использовать один из них в качестве выходного. В результате, путем сравнения параметров трафика, атакующий сможет выделить трафик пользователя до конечного ресурса. Наиболее простым вариантом такой атаки является атака подтверждения, возможная в случае, когда атакующему известны используемые входной и выходной узлы. В таком случае сравнение параметров трафика используется для подтверждения использования пользователем данного соединения.

Для уменьшения вероятности проведения подобных атак могут применяться методы статистического исследования узлов сети TOR. Примером использования является сервис DocTor, отслеживающий группы узлов по времени их первого появления в сети. При появлении большого числа узлов за короткий промежуток времени, сервис отправляет уведомление о возможной попытке проведения атаки Сибиллы, требующей наличия в сети большого числа подконтрольных атакующему узлов. С учетом наличия архива документов состояния сети TOR, возможна реализация подобных проверок на стороне клиента для оценки уровня доверия к узлам TOR, и принятия решения об установления сетевого соединения через выбранные узлы. Такой подход обеспечивает дополнительную защиту от возможных атак.

С целью понижения вероятности успешного проведения атак деанонимизации, предлагается механизм проведения оценки узлов сети TOR на основании информации, доступной из документов состояния сети TOR. На основе ряда параметров, таких, как:

- время начала работы узла;
- время непрерывной работы узла;
- страна расположения узла;
- анонсируемая скорость передачи данных;
- принадлежность к семейству (family);
- используемая версия ПО;
- расположение в дата-центре или в другой сети,
- предлагается оценивать для каждого узла вероятность принадлежности к группе узлов, введенных в сеть для проведения атак пересечения, а также вероятность взаимодействия операторов для пар узлов. Для учета этих оценок при работе с сетью TOR предлагается использование специально разработанной системы управления клиентом сети TOR, выполняющей сбор информации о состоянии сети, вычисление оценок и их использование в алгоритме выбора узлов при установлении сетевых соединений.

Предлагаемый подход к выбору узлов сети TOR перед установлением сетевого соединения на основе информации о состоянии сети и его изменениях позволяет обеспечить дополнительный уровень устойчивости к атакам, направленным на деанонимизацию пользователей.

Новожилов Д.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МЕТРИКИ ДЛЯ АНАЛИЗА СТРУКТУРНЫХ ОСОБЕННОСТЕЙ ВЕБ-СТРАНИЦ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

К настоящему моменту времени в Интернете накоплены значительные объемы информации, обладающей высокой доступностью для пользователей со всего мира. Несмотря на все преимущества, которыми обладает Всемирная паутина, не лишена она и определенных недостатков. В первую очередь, далеко не все веб-сайты являются источниками полезной информации: часть их содержимого по тем или иным причинам оказывается неприемлемым. Вот почему вместе с проблемой защиты информации всё большую и большую актуальность приобретает и другая проблема - повышения защищенности Интернет-пользователей от нежелательной информации. Она включает в себя два основных направления: ограждение несовершеннолетних от нежелательных материалов и блокировку контента, нарушающего законодательство РФ.

Ввиду наличия огромных массивов информации, сформулированная проблема редко решается с помощью просмотра и анализа контента, выполняемых вручную. Как правило, для этой цели применяются различные автоматические системы, способные обнаруживать нежелательное содержимое. Подобные системы могут использовать разные методики, например, искать вхождение ключевых слов или запрещать подключение ко всем сайтам, кроме заранее определенных «белых списков». Еще один вариант заключается в использовании методов машинного обучения (Data Mining). Тогда основная идея будет состоять в переходе к сформулированной в данной области задаче классификации: отнесении веб-сайта к одной из заранее определенных категорий («сайты для взрослых», «алкоголь», «оружие», «наркотики» и т.д.).

Существует множество различных подходов к классификации веб-сайтов. Большинство из них базируется на анализе текстового содержимого, который достаточно эффективен и широко используется. Однако современная веб-страница представляет из себя документ, созданный на стыке многих современных технологий, связанный ссылками с другими аналогичными документами и отличающийся сложностью структуры, информацию о которой также можно использовать в процессе анализа. Это оказывается особенно полезно для целого ряда категорий («чаты», «форумы», «новости»), которые ничем не отличаются по своему текстовому наполнению, в то время как особенности построения у них разные. В таких случаях используют дополнительные признаки, например, анализируют html-тэги их разметки. Данный подход включает в себя различные варианты построения метрик. Все они на начальном этапе формируют список (так называемый «словарь тэгов»), в той или иной степени встречающихся на каждом из сайтов. Этот словарь является своего рода базисом, по которому раскладываются все веб-страницы, а способ назначения коэффициентов определяется метрикой.

Первый и наиболее «наивный» вариант предлагает проверять наличие/отсутствие тэгов разметки на странице. Однако их набор, присутствующий на большинстве веб-страниц, в целом достаточно стабилен. Кроме того, данный подход не учитывает частотные характеристики, а потому не делает различия между тэгами, встретившимися один и десятки раз, что могло бы указывать на сайты различной направленности и улучшить качество категоризации. Аналогичным недостатком обладает и другой вариант, считающий количество каждого тэга из «словаря».

Другой вариант метрики вводит понятие «статистика тэгов», которая определяется как совокупность частот их встречаемости (отношение количества экземпляров данного тэга к общему числу тэгов на странице). Однако данный подход не может исключить зависимость между количеством экземпляров данного тэга и общим числом тэгов на сайте. Поэтому 10 тэгов, отнесенные к 100 и 100 тэгов, отнесенные к 1000, будут давать в данной метрике одинаковый результат, но могут указывать на совершенно разный результат.

Еще один способ построения метрики («нормированная статистика тэгов») может заключаться в следующем: для каждого тэга из «словаря» найти максимальное число его вхождений среди всей выборки, которое затем нормировать, взяв от него, например, 95% (величина, призванная исключить резкие отклонения в количестве тэгов, её точное значение еще предстоит установить экспериментально). На следующем шаге для каждой веб-страницы в выборке подсчитывается отношение числа экземпляров её тэгов из «словаря» к их только что подсчитанным нормированным значениям.

Реализация описанных метрик и последующее проведение экспериментов с ними является текущим направлением деятельности. Предполагается, что данные исследования позволят повысить защищенность пользователей сети Интернет от нежелательной информации.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

В настоящее время в развитии общества защита информации приобретает важнейшее и актуальное значение.

В последние годы быстрыми темпами происходит развитие информационного общества. В информационном обществе владение информацией и всеми методами, формами и средствами ее производства, распространения, хранения, обработки и использования – это ежедневная необходимость и обязанность для каждого члена общества.

Бурное развитие электронных средств массовой информации и социальных сетей привело к широкому обсуждению проблемы конфиденциальности персональных данных пользователей сети «Интернет» во всем мире.

Результатом обсуждения проблемы конфиденциальности персональных данных стало принятие поправок в Закон «Об информации, информационных технологиях и о защите информации»; а также в ряд статей ГПК РФ, в соответствии с которыми гражданам предоставляется так называемое «право на забвение».

В июле 2014 года президентом Российской Федерации В.В. Путиным подписан закон о внесении поправок в федеральные законы №152-ФЗ «О персональных данных» и №149-ФЗ «Об информации, информационных технологиях и о защите информации». Подписанный закон обязал интернет - компании, занимающиеся бизнесом в Российской Федерации (РФ), хранить персональные данные граждан РФ только на серверах, расположенных на территории нашей страны.

С 1 сентября 2015 г. уже вступили в силу дополнения в федеральный закон №152-ФЗ «О персональных данных», обязывающие компании обеспечить обработку персональных данных граждан Российской Федерации в базах данных в России.

В начале августа свою позицию по наиболее острым вопросам применения требования о хранении и обработке персональных данных на территории России высказало Минкомсвязи России – ведомство, уполномоченное осуществлять функции по выработке и реализации государственной политики в области персональных данных.

В частности, Минкомсвязи прояснило, что: кроме российских компаний и представительств/филиалов иностранных компаний в РФ требование о локализации должны исполнять иностранные компании, не имеющие официального присутствия в РФ, но ведущие бизнес через Интернет, направленный на территорию РФ (о чем свидетельствует использование доменных имен .ru, .рф; наличие русскоязычной версии сайта; осуществление расчетов в рублях и пр.); «первичная» база данных может быть в бумажной форме, поэтому требование о локализации будет исполнено, если в России в бумажном виде хранятся персональные данные, которые затем в электронном виде передаются за границу; обработка данных может производиться за границей, если база в РФ является наиболее полной и актуальной (недопустимо нахождение за пределами РФ данных, которые одновременно не находятся в РФ).

Другая проблема требования о локализации персональных данных – это отсутствие эффективных мер ответственности за несоблюдение этого требования, которые бы оправдали для многих компаний высокие расходы на реструктуризацию IT-систем.

Так, например, ст. 13.11 КоАП в настоящее время предусматривает максимальный штраф за нарушение правил обработки персональных данных в размере 10 000 рублей.

К сожалению, принятые в начале года в первом чтении поправки в КоАП, увеличивающие в несколько раз размер ответственности, существенно картину не поменяют.

Введенная с 1 сентября 2015 г. специальная ответственность в виде внесения сайта нарушителя в «Реестр нарушителей прав субъектов персональных данных» и последующей блокировки данного сайта тоже вызывает множество вопросов.

По нашему глубокому убеждению требование о локализации персональных данных россиян может в полную силу заработать только тогда, когда они (требования) прозрачны и едины для всех и будет существовать механизм ответственности, обладающий достаточной побудительной силой для всех компаний.

Отметим особо, что с 1 января 2016 года вступил в силу закон "о праве на забвение". Данное право позволяет гражданину прекратить доступ посредством поисковых систем к видеороликам, фотографиям или любой другой информации о себе, размещенной в сети «Интернет», а также требовать прекращения выдачи ссылок на информацию, распространяемую с нарушением законодательства.

Таким образом, принятые в последнее время требования к обработке персональных данных являются перспективными и позволяют повысить информационную безопасность государства.

Парфенов Н.П., Сударев В.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

НЕКОТОРЫЕ МЕРЫ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Органы внутренних дел (далее в тексте полиция) в своей служебной деятельности обязаны использовать новейшие достижения науки и техники, информационные системы, сети связи, а также передовую информационно-телекоммуникационную структуру (ст. 11 Федерального закона от 07 февраля 2011 г. № 3-ФЗ «О полиции»).

В связи с вышеизложенным, одной из важнейших задач, на современном этапе развития общества, в МВД России является обеспечение защиты информации, в частности защита электронного документооборота в служебной деятельности.

Развитие электронных средств массовой информации и социальных сетей, в частности электронного документооборота, привело к обострению проблемы защиты информации во всем мире, в частности в служебной деятельности органов внутренних дел (ОВД).

Особенно остро эта проблема проявила себя в последние годы. Например, в июле 2014 года Shaltay Boltay взломали почтовый ящик на Gmail.com вице-премьера Аркадия Дворковича и опубликовали его переписку. Подлинность переписки подтвердили газете «Ведомости» два человека, чьи письма были опубликованы.

В августе 2015 года секретарь Совета безопасности России Николай Платонович Патрушев потребовал от руководителей регионов Российской Федерации принять особые меры в отношении чиновников, использующих в служебной деятельности иностранные сервисы Google, Yahoo и Whatsapp. Н.П. Патрушев особо подчеркнул, что применение чиновниками для решения служебных задач ресурсов, расположенных на территории иностранных государств, представляет серьезную опасность.

В марте 2016 года ГУ МВД России по г. Москве запретило передавать служебные сведения через мессенджеры и социальные сети. Под запрет в ГУ МВД России по г. Москве попали Viber, WhatsApp, Skype, Instagram, Twitter, Facebook, «ВКонтакте» и «Одноклассники». Кроме того, в черном списке ведомства оказались электронные ящики на Gmail.com, Mail.ru, Rambler.ru — московские стражи порядка не смогут использовать их для передачи служебной информации.

С целью повышения эффективности организационно-управленческой деятельности ОВД, связанных с документационным обеспечением, в марте 2012 года МВД утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России в 2012-2014 гг.

Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства.

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, который велся с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и госорганами различных уровней.

ИСОД МВД включает интегрированную мультисервисную телекоммуникационную сеть (ИМТС), систему централизованной обработки данных (ЦОД и ПТК), прикладные сервисы обеспечения повседневной деятельности подразделений МВД (повседневные сервисы сервис электронного документооборота (СЭД); сервис электронной почты (СЭП); ведомственный информационно-справочный портал (ВИСП); систему видеоконференцсвязи), прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД (служебные сервисы), а также подсистему поддержки взаимодействия подразделений МВД с населением и межведомственного взаимодействия и подсистему обеспечения (информационной безопасности) ИБ.

Доступ пользователей к сервису электронного документооборота (СЭД) осуществляется исключительно с компьютеров, подключенных к ИМТС.

Подводя итоги рассмотренных вопросов, отметим, что повышение защиты электронного документооборота достигается за счет обеспечения безопасного обмена документами в рамках СЭД, а также за счет обеспечения безопасного хранения и разграничения доступа к информации, включающей журналирование действий пользователей и электронную подпись.

Попова А.Н.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

К ВОПРОСУ О ПОИСКАХ УЯЗВИМОСТЕЙ В ИНТЕРНЕТ-СИСТЕМАХ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Развитие информационный систем неразрывно связано с обеспечением их защиты, а значит и с развитием информационной безопасности. Важно не только организовать хранение объектов интеллектуальной собственности так, чтобы исключить их несанкционированное распространение, но и обеспечить оперативный и удобный доступ и управление ими со стороны авторов и должностных лиц. Ниже пойдет речь о поиске уязвимостей во все более набирающих популярность для этих целей веб-приложениях, т.е. приложениях, где клиентом выступает браузер, а сервером – веб-сервер. Примером может служить организация защиты информации портала международной конференции «EMECS'11 – SeaCoasts XXVI», прошедшей 22-26 августа в Санкт-Петербурге и разработанной в Российском государственном гидрометеорологическом университете.

Логика веб-приложения распределена таким образом, что хранение данных осуществляется, преимущественно, на сервере, а обмен данными происходит по сети, тем самым реализуя модель «клиент-сервер». Клиентская часть реализует пользовательский интерфейс, формирует запросы к нему и обрабатывает ответы. Серверная часть обрабатывает запрос от клиента, выполняет разнообразные операции, формирует веб-страницу и отправляет ее клиенту по протоколу HTTP. Как и во многих других ситуациях, одним из самых эффективных способов поиска уязвимостей

клиентской части – например, в браузере – является фаззинг. Впервые термин появился еще в 1988 году в работе Барта Миллера «The Fuzz Generator» и подразумевает «подсовывание» программе заведомо некорректных или вообще случайных данных, отлавливая моменты, когда программа не сможет их обработать и вылетит. Точки ввода данных в программу могут быть совершенно различными: будь то текстовая строка, введенная через графический интерфейс, бинарные данные из файла или, например, значение поля в каком-нибудь сетевом запросе. Вместо программы может иметь место веб-приложение, какой-либо компонент или даже драйвер. Публичных и действительно работающих инструментов не так много, но одним из таковых является разработка cross_fuzz от Михаила Залевски, сотрудника Google, который с помощью своего инструмента обнаружил и зарегистрировал более ста уязвимостей во всех популярных веб-браузерах, некоторые из которых до сих пор не устранены.

Фаззер выявляет проблемы путем создания чрезвычайно длинных закрученных последовательностей DOM (Document Object Model) - операций, которые затрагивают сразу несколько документов. Сам по себе DOM – это объектная модель документа, позволяющая скриптам и программам получать доступ к содержимому страницы, а также изменять как само содержимое, так и структуру, и оформление документа. Проверяя возвращаемые объекты и вновь рекурсивно используя их, можно создавать круговые зависимости узлов, с помощью которых становится возможным применить своеобразный стресс-тест для механизмов сборки мусора браузера. Таким образом проверяется способность приложения к правильному и эффективному освобождению памяти для более неиспользуемых объектов. Это так называемые use-after-free уязвимости, связанные с алгоритмом «garbage collection». Код фаззера написан на HTML/ JavaScript, поэтому для поиска уязвимостей с его помощью достаточно открыть нужный HTML файл в браузере.

Так как большинство веб-сервисов, используемых для управления документооборотом, а также конфиденциальными данными пользователей, написаны с применением языка PHP, то в этом случае при поиске уязвимостей необходимо обратить внимание на взаимодействие алгоритма «сбора мусора» с другими объектами PHP и на уязвимые функции сериализации/десериализации, которые могут обрабатывать, к примеру, информацию, загружаемую пользователями, так как десериализация и user input сочетаются очень плохо.

Таким образом, применяя данный метод анализа веб-приложения возможно получить достоверную оценку его уязвимостей для своевременного их устранения и обеспечения безопасного хранения конфиденциальных данных и объектов интеллектуальной собственности при проведении научных конференций.

Проноза А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

АНАЛИЗ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ БОЛЬШИХ ДАННЫХ ДЛЯ РЕШЕНИЯ ЗАДАЧИ МОНИТОРИНГА КРУПНОМАСШТАБНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Одной из множества задач, для решения которых необходимо собирать и обрабатывать большие массивы информации, является задача получения актуальной информации о состоянии безопасности крупномасштабной вычислительной сети. Решение этой задачи является одной из ключевых функций подсистемы визуализации системы управления событиями и информацией безопасности (Security Information and Event Management – SIEM).

В процессе анализа состояния безопасности компьютерной сети подсистема визуализации собирает данные от различных ее источников (систем обнаружения вторжений, брандмауэров, журналов работы программных и аппаратных средств, анализаторов сетевого трафика и т.д.). Поскольку каждый источник порождает сообщения безопасности о событиях, происходящих в сети, в свойственном только ему формате, на выходе получаются большие массивы разнородной слабоструктурированной информации. В силу размеров современных вычислительных сетей и числа возникающих в них событий количество таких сообщений постоянно возрастает. Следовательно, можно утверждать, что подсистема визуализации SIEM-системы имеет дело с обработкой и анализом больших данных.

Основной задачей подсистемы визуализации является построение графического изображения, наглядно представляющего пользователю информацию о текущем состоянии безопасности объекта визуализации. Таким образом, в современных SIEM-системах возникает необходимость визуализации в режиме реального времени результатов сбора и обработки больших данных с целью отображения состояния безопасности компьютерной сети.

Процесс визуализации в SIEM-системе состоит из выбора наиболее подходящей модели визуализации, заполнении ее атрибутов значениями, полученными в результате обработки всего массива сообщений безопасности, и вывода изображения. Выбор конкретной модели визуализации должен основываться в том числе на принципе соотношения информативности и эффективности, т.е. какое максимальное количество информации способно передать итоговое изображение человеку, задействовав

минимально его когнитивный аппарат. При выборе и анализе моделей визуализации больших данных представляется целесообразным исследовать, какие именно из их характеристик – объем (volume), разнообразие (variety) или скорость возникновения (velocity) – они способны наглядно отобразить.

Для визуализации больших данных исследователи выделяют ряд моделей, которые также применимы и для данных в их традиционном понимании. К таким моделям относят «солнечные лучи» (Sunburst), круговая сетевая диаграмма (Circular Network Diagram), параллельные координаты (Parallel coordinates) и потоковые графы (Streamgraph). Приведенные модели можно разбить на классы в соответствии с тем, какие именно характеристики больших данных они способны визуализировать. Так, «солнечные лучи» и потоковые графы наглядно представляют объем и скорость возникновения данных, круговая сетевая диаграмма отображает их объем и разнообразие, а модель на параллельных координатах способна отобразить все три характеристики.

Заметим, что не все традиционные модели визуализации, применимые для визуализации компьютерной инфраструктуры, подходят для эффективного представления больших данных. Например, такая распространённая модель, как карты деревьев (Treemap), способна отобразить лишь объем данных.

Все указанные модели могут применяться в современных SIEM-системах для представления различных аспектов безопасности компьютерной сети, таких как ее топология, объем сетевого трафика, направления компьютерных атак, настройки политик безопасности и т.п.

В докладе более подробно рассматриваются модели визуализации, используемые в SIEM-системе, и делается попытка адаптировать классические модели для отображения результатов обработки больших данных.

Приведенный подход к анализу множества моделей визуализации больших данных путем его разбиения на классы может быть расширен, если принимать во внимание характеристики больших данных, которые они приобретают с течением времени – изменчивость (variability), достоверность (veracity) и ценность (value). Данные характеристики потребуют от модели визуализации способности оперативного отклика на непрерывно поступающие новые данные, возможности автоматической коррекции изображения и нового уровня интерактивности. В рамках SIEM-системы это означает увеличения скорости реагирования пользователя на инциденты безопасности, возникающие при работе в крупномасштабных вычислительных сетях.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Проноза А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВИЗУАЛИЗАЦИИ БОЛЬШИХ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Эффективная визуализация огромных массивов данных является одной из наиболее востребованных задач на сегодняшний день. Применительно к компьютерной инфраструктуре в качестве таких массивов будем рассматривать сообщения безопасности, возникающие в крупных компьютерных сетях, которые, в силу их количества, разнородности и высокой скорости генерации, представляют собой большие данные. Функция визуализации сообщений безопасности в компьютерных сетях возлагается на подсистему визуализации, являющейся частью системы управления информацией и событиями безопасности (SIEM).

Наиболее наглядной и широко распространенной моделью визуализации компьютерной сети является граф. Однако в случае крупных сетей и интенсивного потока сообщений безопасности данная модель обнаруживает ряд недостатков. Вывод большего количества объектов (рабочих станций, серверов, коммутационного оборудования и т.п.) требует большей поверхности отображения, а применение алгоритмов фильтрации и агрегации, таких как, например, вывод только уязвимых хостов или объединение хостов в подсети, становится причиной частичной потери информации. При визуализации больших сетей неизбежно возникает необходимость отображения большого числа связей (физические каналы связей, функциональные зависимости, отношения компрометации и т.п.), в результате чего часто появляется визуальный шум. Проблемы визуализации компьютерной сети в виде графа заключаются, прежде всего, в недостаточной поверхности отображения и ограниченности когнитивных способностей человека.

Большой поток сообщений безопасности приводит к постоянному изменению ситуации и, пока пользователь исследует визуализацию, состояние безопасности компьютерной сети может измениться. Наличие большого количества данных может привести к низкой производительности процессов интерактивной визуализации, поскольку ответ на запрос пользователя заставит подсистему визуализации заново отбирать и обсчитывать значения атрибутов запрашиваемой модели.

Большие данные отличает от данных в традиционном понимании отсутствие четкой структуры, многомерность и многокатегориальность хранимой информации. В связи с этим возникает потребность в разработке алгоритмов понижения размерности данных. Так, например, при подготовки к отображению компьютерных сетей целесообразно стоить многомерную матрицу связей между ее объектами, а в качестве результата визуализации рассматривать только ее срезы по виду связи. Другим следствием многомерности данных является необходимость поддержки подсистемой визуализации нескольких различных моделей представления (карты деревьев, параллельные координаты, солнечные лучи и т.п.).

Среди других особенностей больших данных следует отметить необходимость определения их ценности (value) и достоверности (veracity). Ценность отображаемых данных заключается в том, чтобы сфокусировать внимание пользователя на проблемных участках сети. К достоверности можно отнести, например, способность SIEM-системы отличать целевые кибернетические атаки от случайных. Такие характеристики, как ценность и достоверность, могут стать «естественным» фильтром при подготовке визуального представления.

Большой объем сообщений и ограниченная пропускная способность каналов передачи данных зачастую делают невозможным расчет значений атрибутов модели визуализации на специально выделенном оборудовании. Процесс подготовки визуального представления большого количества сообщений безопасности вынужден повторять концепцию их обработки, согласно которой не сообщения передаются подсистеме визуализации, а алгоритм работы подсистемы переносится к хранимым на хостах сообщениям. Таким образом, процесс построения визуализации может носить распределенный характер.

В докладе более подробно рассматриваются проблемы визуализации больших данных в существующих SIEM-системах с точки зрения разработки распределенного алгоритма построения модели визуализации и заполнения значениями ее атрибутов. Для получения практических результатов разворачивается стенд, в котором анализ сообщений безопасности будет организован согласно модели MapReduce, а сами сообщения будут обрабатываться отдельно на каждом источнике информации (вычислительном узле).

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Резединова Е.Ю., Кожушко Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

МЕТОДЫ СЕНТИМЕНТ-АНАЛИЗА ВЫСКАЗЫВАНИЙ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ TWITTER

Растущая популярность социальных сетей и числа их пользователей приводит к накоплению огромных объемов информации, которая может быть подвергнута автоматизированному анализу. Практически каждое событие находит отражение в социальных сетях через реакции людей. События легко могут вызвать общественный резонанс, невероятно быстро распространившись по социальным сетям и охватив значительные пласты общества. В связи с этим актуальной представляется задача систематизации и анализа сообщений, содержащих отклик пользователей социальных сетей на те или иные события с целью прогнозирования возможных сценариев и последствий развития ситуации.

Микроблоггинговая платформа Twitter представляет собой социальную сеть, где в виде ленты новостей отображаются сообщения пользователей, ограниченные длиной в 140 символов. Актуальные темы и ключевые слова в своем большинстве выделяются знаком «#», который позволяет осуществлять быстрый поиск. Наиболее актуальные темы выносятся на сайте в отдельную таблицу, что позволяет следить за изменением трендов.

Ограничение на размер сообщения побуждает пользователей подбирать для своих сообщений наиболее эмоционально окрашенные слова и выражения, с тем, чтобы в условиях небольшого количества символов ярче и полнее выразить свое отношение к какому-либо событию или явлению.

Иными словами социальные сети являются идеальной средой для Text Mining – поиска, обработки и анализа текстов, в которых содержатся как персональные данные пользователей, так и их мнения и суждения относительно определенного события.

В связи с изложенным весьма актуальным представляется создание программного комплекса, позволяющего проводить сентимент-анализ (sentiment analysis) высказываний пользователей, определять их отношение к тому либо иному событию или явлению с целью получения общей картины уже произошедших событий и прогнозирования на ее основе дальнейшего развития ситуации. В качестве промежуточных задач в данном случае можно выделить следующие:

1) Изучение приемов, позволяющих расширить возможности анализа текстов.
2) Изучение opensource решений для данной области.
3) Изучение методов машинного обучения.
4) Изучение возможностей прогнозирования.

Романова Ю.Н., Янюшкин К.А., Ныpков А.П.
Россия, Санкт-Петербург, Университет ИТМО, ГУМРФ им. адм. С.О. Макарова
О ПРИМЕНЕНИИ ОТЕЧЕСТВЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Пару десятилетий назад криптография в России использовалась только военными и спецслужбами, поэтому находилась под полным контролем государства и никакие научные работы по криптографии не могли быть опубликованы для широкого круга лиц. Только в 1994 году был впервые открыто опубликован стандарт ГОСТ 28147-89, описывающий процесс блокового шифрования с симметричным ключом. С этого времени отечественная криптография начинает своё публичное развитие, появляется множество материалов с описаниями алгоритмов и протоколов, криптоанализом и всем, что с этим связано. Сегодня кроме зарубежных алгоритмов шифрования в России используются собственные разработки в области информационной безопасности: алгоритмы шифрования, программы и программно-аппаратные комплексы, которые эти алгоритмы используют. Рассматривая некоторые российские стандарты, а так же некоторые популярные зарубежные аналоги, можно прийти к выводам, что существующие теоретические атаки незначительно снизили практическую криптостойкость отечественных алгоритмов шифрования. Вычислительных ресурсов требуется такое огромное количество, что значительную часть шифруемой информации расшифровывать будет просто экономически невыгодно, а для сведений особой важности существует класс идеально стойких систем шифрования. Серьезную угрозу подавляющему большинству асимметричных криптографических схем, в том числе и отечественной схеме цифровой подписи, может представлять появление мощных квантовых компьютеров. Впрочем, перспективы их создания представляются неясными.

Резединова Е.Ю., Ушанова И.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПОДБОР ФОРМАЛЬНЫХ ПРИЗНАКОВ ДЛЯ АВТОМАТИЗАЦИИ ПОИСКА БОТОВ В СОЦИАЛЬНЫХ СЕТЯХ

На примере страниц предполагаемых ботов в различных социальных сетях выделяются и рассматриваются признаки, позволяющие отличить страницу реального пользователя от бота.

Сегодня социальные сети являются одной из основных составляющих общественной жизни. Информация, опубликованная на каком-либо ресурсе, практически мгновенно становится доступной для прочтения и дальнейшего тиражирования на любой сетевой платформе.

В тоже время довольно часто встречающимся явлением становится создание и распространение информации так называемыми ботами, осуществляемое в рекламных целях, для дезинформации или формирования определенного общественного мнения.

В связи с этим создание программы, позволяющей автоматизированным способом производить отслеживание ботов в социальных сетях, является актуально задачей, для решения которой в том числе необходимо определить, на основании каких формальных признаков это можно сделать.

С этой целью авторами были изучены такие распространенные социальные сети как: Вконтакте, Twitter, Facebook, Instagram, Одноклассники. Для каждой из названных сетей характерны определенные виды ботов. В частности, для Вконтакте, Facebook и Одноклассников – это, прежде всего, чат-боты, в Twitter - коммерческие боты, рекламирующие товары или услуги. В Instagram присутствует большое количество ботов, работающих с аккаунта реального пользователя и рассылающих предложения о работе в сетевых пирамидах в комментариях под фото и видео сообщениями.

В тоже время можно выделить общие признаки, наличие которых с большой вероятностью указывает, что рассматриваемая страница управляется ботом, а именно:

1. Существенное превышение числа подписчиков над количеством друзей данного пользователя.

2. Значительное преобладание записей-репостов над «живыми» записями.

3. Необходимость внесения платы за возможность общения со страницей пользователя (переписка, комментарии и т.д. – в зависимости от особенностей социальной сети), о чем прямо указывается в одном из первых постов. Как правило, в этом случае имеется ссылка на интернет-магазин или другие контактные данные.

4. Отсутствие на странице фото-, аудио-, видеоконтента и(или) однообразие контента, дата появления которого, как правило, совпадает с датой создания самой страницы.

5. Наличие явной прослеживаемой периодичности появления публикаций на странице (например, раз в несколько дней создается n записей, с разницей в несколько минут).

6. Выраженная устойчивость структуры большинства публикаций (повторяющиеся ключевые слова, наличие определенных ссылок, изображений и т.д.).

7. Отсутствие (за исключением необходимого минимума) личной информации о пользователе страницы либо заведомо недостоверная информация (например, использование чужого имени или фотографии).

8. Присутствие в подписках большого количества официальных страниц публичных персон, организаций, магазинов, СМИ и прочего.

9. Наличие значительного количества комментариев под публикациями известных людей и групп, появляющихся почти мгновенно или через небольшой промежуток времени после публикации.

Использование названных признаков даст возможность автоматически опознавать страницы в социальных сетях, управляемые ботами, что в свою очередь позволит «отсеивать» нежелательные публикации, предотвращать захламление интернет-пространства, блокировать соответствующие страницы, вычислять источники формирования информационных поводов и мнений и т.д.

Саенко И.Б., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МОДЕЛИ И МЕТОДЫ ВИЗУАЛЬНОГО АНАЛИЗА СХЕМ И ПОЛИТИК РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Единое информационное пространство (ЕИП) в настоящее время является перспективным и динамично развивающимся научным направлением в области информационного обеспечения больших корпоративных информационно-коммуникационных систем (сетей). Однако, несмотря на то, что тематика построения ЕИП широко рассматривается в отечественной и зарубежной литературе, многие аспекты данного направления, включая вопросы построения системы разграничения доступа в информационном пространстве, остаются либо недостаточно изученными, либо изученными только для отдельных конкретных областей их реализации.

Одной из составляющих проблемы построения системы разграничения доступа к ресурсам ЕИП является необходимость разработки моделей и методов их анализа, в частности, их визуального анализа. Специфика данных моделей и методов обусловлена тем, что визуальный анализ позволяет значительно быстрее обнаружить конфликты или противоречия в политиках безопасности, чем формальные модели и методы, за счет использования возможностей человека по обработке информации, воспринимаемой зрительным путем.

К разработанным моделям и методам визуализации схем и политик разграничения доступа к ресурсам ЕИП предъявлялись следующие требования: 1) возможность кластеризации больших массивов данных; 2) возможность автоматической классификации массивов данных; 3) возможность «ленивой» загрузки массивов данных при визуализации; 4) возможность детализации кластеризованных данных (Drill-down); 5) возможность микширования данных (mesh-up) при их визуализации.

В качестве основного алгоритма кластеризации был использован алгоритм CLOPE (Clustering with sLOPE). Этот алгоритм обеспечивает более высокую производительность и лучшее качество кластеризации в сравнении со многими иерархическими алгоритмами. Достоинствами алгоритма CLOPE являются: а) его высокая масштабируемость и скорость работы, а также качество кластеризации; б) алгоритм CLOPE автоматически подбирает количество кластеров, причем это регулируется одним единственным параметром - коэффициентом отталкивания.

Предложенные модели и методы автоматической классификации обеспечивают обработку полуструктурированных и неструктурированных данных. Обработка полуструктурированных данных осуществляется на основе алгоритмов Naïve Bayes и Decision Tree, базовые предсказания которых объединяются на верхнем уровне с помощью алгоритма Stacking. Обработка неструктурированной информации осуществляется с помощью системы многоуровневых предсказаний о принадлежности описаний объектов нижнего уровня к одной из целевых категорий верхнего уровня.

Под термином «ленивая» загрузка (lazy loading) понимается способ загрузки данных для создания характеристики объекта или совокупности связанных объектов, позволяющий отсрочить инициализацию объекта (объектов) до момента времени, в котором это необходимо. Реализация «ленивой» загрузки при визуализации данных обладает следующими преимуществами: а) повышение наглядности визуального представления; б) возможность использовать в качестве исходных данных при визуализации потоки данных (применение таких операторов потоковой обработки, как Filter и Map, позволяют, с одной стороны, уменьшить интенсивность потока данных, а с другой – исключить несущественные характеристики).

Под термином Drill-down («проникновение вниз») понимается метод анализа информации в хранилищах данных, предусматривающий пошаговый переход к более низким уровням иерархии элементов измерений для получения более детальных сведений об исследуемых процессах или явлениях. Метод Drill-down позволяет осуществлять анализ в направлении последовательного увеличения уровня подробности рассматриваемых данных.

Микширование как процесс обработки данных применительно к визуализации информации означает наложение друг на друга графических моделей, выполняемое с целью визуального анализа связей и закономерностей, имеющихся между данными, и повышения выразительности визуальных представлений для лица, принимающего решения.

Разработанные модели и методы визуализации схем и политик разграничения доступа к ресурсам ЕИП, отвечающие перечисленным выше требованиям, были реализованы в следующих способах: 1) визуализация с использованием GIS-систем; 2) инфографика; 3) табличные способы; 4) иерархические способы.

Экспериментальная оценка предложенных моделей и методов визуализации показала их достаточно высокую эффективность. Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем №№ 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Саенко И.Б., Кушнеревич А.Г., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»

ПЛАТФОРМА ПАРАЛЛЕЛЬНОГО РАСПРЕДЕЛЕННОГО АНАЛИЗА ТРАФИКА В КОМПЬЮТЕРНЫХ СЕТЯХ ДЛЯ ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

Объемы передаваемых данных в сетях уже сегодня достигают таких величин, что традиционные методы обработки и хранения данных перестают удовлетворять требованиям к быстродействию таких систем. По мере увеличения объемов обрабатываемой информации до недавнего времени применялось только вертикальное масштабирование вычислительных ресурсов систем обработки, когда увеличение производительности достигается за счет покупки более дорогостоящего и мощного оборудования в замену старому. Производительность современного оборудования растет намного медленнее, чем объемы данных для обработки, поэтому вертикальное масштабирование исчерпало себя. Чтобы снизить материальные затраты и повысить эффективность использования устаревающего оборудования были разработаны системы и методы консолидации вычислительных ресурсов множества машин. Такой метод увеличения производительности системы, за счет добавления к ней нескольких машин вдобавок к уже задействованным, называется горизонтальным масштабированием. Подход горизонтального масштабирования позволяет неограниченно увеличивать производительность системы обработки, однако требует специального подхода к написанию программ в параллельном исполнении.

Особенно остро в компьютерных сетях стоит вопрос мониторинга безопасности, который заключается в сборе и предварительной обработке больших массивов гетерогенных данных о событиях и обнаружения инцидентов безопасности. При этом сбор и предварительная обработка данных мониторинга безопасности должна выполняться «на лету», путем обработки потоков данных. Для этой цели разработана программная платформа, обеспечивающая распределенную потоковую обработку данных о событиях безопасности на основе подхода Complex Event Processing (CEP).

Подход CEP, лежащий в основе обработки потоков данных, предполагает, что над потоками данных можно выполнять некоторую совокупность операций по аналогии, как в реляционных базах данных выполняются операции над таблицами данных. При этом каждый поток данных воспринимается как следующие друг за другом записи (кортежи) данных, имеющие одинаковую схему. Схема записей данных является также схемой потока данных.

Разработанная платформа ориентирована на выполнение следующих потоковых операций: отображения Map, фильтрации Filter, объединения Union, агрегации Aggregate и соединения Join. Операция Map является аналогом реляционной проекции, Filter – селекции, Union – объединения, Join – соединения. Действия, выполняемые операцией Aggregate, аналогичны действиям по инструкции GROUP BY в языке SQL.

На данный момент стандартом в области распределенных вычислений является система Hadoop, хотя в последнее время широкую популярность приобретает система Spark. В силу того, что основой Hadoop является вычислительная модель MapReduce, любой алгоритм для Hadoop состоит из двух методов, а именно: mapper и reducer. К тому же, необходим еще и третий метод task, который запускает задачу. Из-за этого программный код, написанный при подходе MapReduce, является громоздким и сложно читаемым. Система Spark использует свою вычислительную модель, основанную на RDD-блоках. В результате программный код для Spark на порядок короче, чем для Hadoop, и состоит всего из одного метода. Кроме того, запись данных на жесткий диск в Spark выполняется не так часто, как в Hadoop (в Hadoop она выполнятся при каждом выполнении операции Map). При этом Spark больше и эффективнее использует оперативную память машины, что выливается в более высокую скорость работы и выигрыш на итеративных алгоритмах до 100 раз по оперативной памяти и до 10 раз по требуемому пространству на жестком диске.

Структура разработанной платформы включает в себя следующие модули: 1) сбора данных; 2) агрегации данных; 3) нормализации и анализа данных; 4) визуализации данных; 5) работы с хранилищем данных. Модули агрегации, анализа и работы с хранилищем реализованы с использованием библиотек параллельных потоковых вычислений Hadoop и Spark, которые поддерживают подход CEP. Комплекс модулей развернут на платформе виртуализации, что обеспечивает необходимые мобильность и гибкость управления системой. Модуль визуализации

использует стандартные графические модели (графики, круговые диаграммы, гистограммы и т.д.) и нестандартные (карты деревьев, матрицы, диаграммы Вороного, графы с глифами и т.д.). Исходные данные для визуализации хранятся в промежуточной базе данных.

Экспериментальная оценка показала достаточно высокую производительность платформы при обработке больших массивов данных о трафике компьютерной сети.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).

Саликов А.В.
Россия, Санкт – Петербург, Санкт-Петербургский Университет МВД России

БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

С развитием информационных технологий, а также с популярностью передачи информации через сеть Интернет, возникает необходимость защиты данных пользователя во «Всемирной паутине». Дело в том что, в вопросах связанных с безопасностью своих персональных данных преобладает большое количество людей с низким уровнем знаний в данной сфере. Для того чтобы зарегистрироваться в социальных сетях, пользователи используют свои личные данные, предоставляя администратору данной сети сведения о себе, а также свое имя, фамилию и отчество, адрес электронной почты, свой контактный телефон, место жительства и другу информацию, связанную с личными данными.

Однако кроме этого, пользователь ставит галочки, в пустом поле электронной регистрации, в котором содержится соглашение с правилами и условиями обработки предоставленных пользователем сведений о себе.

Руководствуясь статьей. 9 части 1 Федерального закона "О персональных данных" пользователь решает, предоставлять свои данные третьему лицу либо нет. В случае согласия по предоставлению сведений он дает согласие на переработку своих данных.

Пользователь персональных данных при регистрации на интернет-сайте, принимает условия, которые предлагает ему владелец интернет-сайта (пользовательское соглашение) и тем самым обязуется соблюдать_эти_соглашения.

В случае утраты пароля, а также при любой невозможности автоматизации этого пароля на сайте, пользователь имеет право обратиться в администрацию данного сайта, либо в разделе «Помощь» и следовать дальнейшим инструкциям. Для восстановления учетной записи, администрация сайта имеют право потребовать изменить, дополнить, придумать новый пароль пользователя на данном сайте.

Для того чтобы восстановить пароль, в случае утраты доступа к учетной записи пользователя, в разделе «Помощь», отправляется СМС - сообщения на контактный номер телефона, который пользователь указывает при регистрации. После чего на указанный номер телефона присылается СМС – сообщение с кодом для разблокировки персональной страницы пользователя. В таком случае, сайт не нарушает положения законодательства Российской Федерации, в области персональных данных.

Одной из главных задач законодательства Российской Федерации в области «персональных данных» не допустить, что бы сведения о субъекте персональных данных попала злоумышленникам.

Существуют сайты, где отсутствует графа, в которой указывается согласие пользователя на обработку его персональных данных, тем самым нарушая требование конфиденциальности установленные законодательством Российской Федерации.

В случае обращения о правомерности получения сведений о пользователе, владельцы сайтов ссылаются на то, что данная информация была получена в телефонном справочнике, который является общедоступным и приобретена в книжном магазине. В таком случае администратор должен предоставить сведения, в котором субъект персональных данных дает письменное согласие на размещение его персональных данных. Если такие сведения отсутствуют, то владельца сайта можно привлечь к административной ответственности, в зависимости от степени и характера причиненного вреда согласно ст. 13. КРФоАП - нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах.

В таких ситуациях пользователь может обратиться в суд для восстановление своих законных прав. Одной из возложенных задач Роскомнадзора состоит в том, чтобы предупреждать, выявлять, прекращать деятельность интернет-сайтов, которые незаконно распространяют данные о пользователе, тем самым нарушая его законные права. Главным свидетельством борьбы Роскомнадзора со злоумышленниками является практика, она показывает, что по решению суда, по требованию данного государственного органа были удалены персональные данные с различных интернет - ресурсов, а также многие интернет-ресурсы, по решению суда заканчивали свою деятельность.

Помимо этого, были выявлены сайты, которые предлагали возможность выхода к персональным данным, взамен просили отправление СМС-сообщение. По ним было заведено дело по факту мошенничества.

Немаловажную роль играет сотрудничество с партнерами иностранных государств по защите персональных данных в сети Интернет. Имеются положительные результаты совместной, проделанной работы. В дальнейшем Роскомнадзором, планируется модернизировать подход для реализации возложенных на него функций, для достижения высокого уровня.

Главное, о чем пользователь не должен забывать, это о том, что при регистрации в сети Интернет, за предоставленные им данные, сведения, информацию он несет персональную ответственность.

Стахно Р.Е., Ковалёв В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

К ВОПРОСУ О ЗАЩИТЕ ПОТОКОВ ДАННЫХ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается.

В связи с этим понятие «защита информации» становится ключевым и рассматривается как процесс или деятельность, направленная на предотвращение утечки защищаемой информации, а также различного рода несанкционированных воздействий на информацию и ее носители.

Проблемы с защитой информации, как и источники угроз, по своей сущности различные, поэтому возникает необходимость в создании дифференцированных видов ее обеспечения.

Классифицировать средства обеспечения защиты информации можно на несколько групп:

1. аппаратные (технические) средства; 2. программные средства; 3. контаминированные средства; 4. организационные или административные средства.

К аппаратным (техническим) средствам относятся разные устройства. Они могут быть электронными, механическими или электромеханическими, но специфика их работы предполагает защиту информации посредством аппаратных средств. Применение этих устройств позволяет воспрепятствовать физическому проникновению или замаскировать данные, если доступ все же был открыт. Технические средства надежны, независимы от субъективных факторов и обладают высокой устойчивостью к модификации. Но и они обладают рядом недостатков, таких как высокая цена, они недостаточно гибкие и практически всегда обладают большими массой и объемом.

Программные средства позволяют контролировать доступ, проводить идентификацию пользователей, тестировать контроль системы защиты информации. Кроме того, средства, относящиеся к этой группе, могут шифровать данные и удалять рабочую (остаточную) информацию (вроде временных файлов).

Для обеспечения необходимой секретности информации применяют математические методы обеспечения конфиденциальности – криптографию или шифрование информации. При создании зашифрованных данных используют определенный алгоритм или устройство, которое его реализует. Изменяющийся код ключа осуществляет управление шифрованием. Именно с его помощью можно извлечь информацию.

Среди классических алгоритмов, которые используются, выделяют несколько основных:

1. Подстановка. Она может быть, как самой простой, одноалфавитной, так и многоалфавитной сложной (однопетлевой и многопетлевой).

2. Перестановка. Различают простую и усложненную.

3. Гаммирование. Речь идет о смешивании, в котором могут использовать длинную, короткую, неограниченную маски.

В первом случае исходный алфавит заменяется альтернативными. Это самый легкий способ шифрования. Данные, зашифрованные алгоритмом перестановки, будут более защищенными, ведь в нем используются цифровые ключи или эквивалентные слова.

Система, отдавшая предпочтение гаммированию, получит гарантию надежности и безопасности информации, потому что для осуществления этого способа шифрования будет проведена серьезная криптографическая работа. Для защиты используются нелинейные преобразования данных, методы рассечения-разнесения, компьютерная стеганография и прочее.

Контаминированные средства сочетают в себе свойства аппаратных (технических) и программных средств.

К организационным или административным средствам относят средства защиты информации организационно-технического и организационно-правового характера. К ним относят:

- контроль доступа в помещения, их подготовку и оснащение;
- разработку стратегий безопасности организации;

- подборку и изучение национальных законодательств с последующим их применением;
- учреждение правил работы и контроль их соблюдения.

Полноценная защита информации может быть достигнута при использовании всех этих средств в комплексе.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтомуобеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Супрун А.Ф., Туманов Н.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА ИНФОРМАЦИИ ВЫСОКОЙ СТЕПЕНИ ЗАЩЕННОСТИ

В современных условиях продолжает существовать проблема абсолютной защищенности закрытых сетей от внешних угроз. Причиной этому является продолжающееся совершенствование методов и методик создания угроз с целью проникновение в закрытые сети. В настоящее время достаточно хорошо изучен вопрос о несостоятельности межсетевых экранов в борьбе с разнообразными и все более изощренными современными угрозами. Технические способы, позволяющие значительно улучшить защищенность режимных сетей – это однонаправленные шлюзы, значительно усложняющие возможность внедрения в закрытую сеть за счет использования алгоритмов упреждающей коррекции ошибок. Однако полное закрытие каналов внедрения такие шлюзы не обеспечивают. Существует вероятность внедрения через вредоносную или стеганографическую закладку. Стоит отметить, что 100% обнаружение вредоносного кода является теоретически неразрешимой задачей.

На современном рынке представлено множество отечественных и зарубежных комплексов однонаправленной передачи информации. К ним следует отнести варианты однонаправленных шлюзов серий «СТРОМ» и «З-Кросс» обладающих хорошими характеристиками по скорости передачи данных, существенно осложняют проникновение во внутреннюю закрытую сеть, но не устраняющие возможность проникновения полностью даже при использовании оптического канала связи с закрытым сервером.

Следует заметить, что усиленными темпами продолжается развитие методов и способов как снятия информации с оптоволокна так и несанкционированное воздействие на сервер по оптоволокну.

Для гарантированной передачи информации из открытых источников в защищенные сети на сегодняшний день могут служить так называемые АПК (аппаратно-программные комплексы) основанные на механизме оптического сканирования. Однако, скорость передачи информации при использовании этого метода низкая.

Для получения высоких скоростей передачи предлагается использовать принцип оптронной передачи информации по каждому пиксельному модулю. Такие устройства требуют совершенно иного подхода к конструкции матрицы мониторов однонаправленной связи. Необходима замена каждого пиксельного модуля на оптронный модуль, который способен однонаправлено передать степень свечения каждого пиксельного модуля с высочайшей точностью. Таким образом, возможно полное разделение сетей, открытой и закрытой. Заметим, что полностью устраняется возможность обратной передачи информации, т. к. нет связи между закрытыми и открытыми серверами по цепям питания, каналам управления и др. каналам. Только в такие системы шлюзов можно считать однонаправленными в полной мере.

Управление такими аппаратно-программными комплексами может осуществляться с помощью ПЛИС, что обеспечит высокие скорости считывания, кодирования и раскодирования информации. Звуковой канал передачи формируется при необходимости.

Реализация таких структурных схем дает возможность осуществить однонаправленную передачу информации из открытых сетей в закрытые сети без проникновения любых вредоносных программ и без съема информации из закрытых сетей.

Теплов Э.П., Кардакова М.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

АКТУАЛЬНЫЕ ВОПРОСЫ СОЦИОКУЛЬТУРНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С СИСТЕМНЫХ ПОЗИЦИЙ

Исследование проблем информационной безопасности с позиций системной методологии позволяет описывать в доступных понятиях и такую сферу этой безопасности, которая связана не только с «аппаратной» (технической и программной) ее составляющей, но и с самим субъектом этой безопасности. При этом под социальными субъектами подразумеваются различные био-социо-

культутрные системы. От неделимой (единичной, человек) до сложно-составной (всеобщей, человечество).

И в этой связи «социокультурная» информационная безопасность социального субъекта с системных позиций и в операциональном смысле этого понятия может быть представлена как способность социального субъекта планировать и осуществлять различные защитные мероприятия по сохранению своих целей, индивидуальности физического и духовного (физическую индивидуальность, национальную идентичность, мировоззрение, мыслительные, интеллектуальные способности и достижения) состояния (как системы) и возможностей саморазвития в условиях воздействия на него информационных угроз социокультурного характера.

С учетом этого, мы полагаем, защита социокультурной составляющей информационной безопасности социального или политического (госаппарат, партия, общественно-политическое движение) субъекта в операциональном плане может быть представлена как сведенные самим субъектом во взаимосвязанную систему организационно-управленческие, кадровые, финансовые, информационно-программные и материально-технические (включая и «аппаратно-технические») мероприятия, которые способны своевременно:

1) выявлять информацию социокультурного характера, угрожающую его выживанию и развитию;

2) предотвращать воздействие на себя таких информационных угроз;

3) минимизировать разрушительный потенциал реализованных информационных угроз;

4) относительно быстро устранять разрушительные последствия (ущерб) воздействия этих угроз на свою социокультурную сферу;

5) упреждающе воздействовать (атаковывать!) на источник информационной угрозы и ее содержание, предупреждая и опережая враждебные социокультурные информационные операции, атаки и диверсии.

Усов Е.С., Никольский А.В., Павленко Е.Ю., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ОБЛАЧНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ INTEL SGX

За последние пять лет современные высокопроизводительные системы стали доступны пользователям сети Интернет в связи с активным развитием технологии облачных вычислений. Данная технология позволяет пользователю хранить и обрабатывать информацию в современном центре обработки данных, оснащенном высокопроизводительным оборудованием и разнообразным программным обеспечением. При этом, управление данными процессами возможно с любого персонального устройства, имеющего доступ к сети Интернет, без учета его аппаратных и программных ресурсов. Подходы и методы, лежащие в основе технологии облачных вычислений, позволяют согласовать одновременную работу сотен тысяч программ и приложений, тысяч операционных систем и сотен компьютеров и получить решение, обладающее новыми качествами – эластичностью, оперативным выделением вычислительных ресурсов по требованию и высокой оперативной доступностью посредством Интернет.

Необходимость обеспечения защиты персональных данных пользователей облачных технологий является важной и актуальной задачей, в связи с огромным количеством людей, использующих различные облачные сервисы. Основной проблемой безопасности в облачных вычислениях является зашита данных пользователя от атак провайдера облачных услуг. Данная проблема может быть успешно решена с использованием гомоморфного шифрования с открытым ключом. Данный подход предоставляет возможность проведения операций над зашифрованными данными в облаке и гарантирует, что никто, кроме владельца данных, не сможет получить доступ к ним. Однако, в настоящее время гомоморфное шифрование не позволяет выполнять произвольные вычисления над зашифрованными данными, а также обладает низкой производительностью, что делает невозможным его использование в облачных вычислениях.

Решением вышеописанной проблемы обеспечения безопасности систем облачных вычислений может стать аппаратная технология, способная защитить данные пользователей облачных услуг на самом низком уровне. В процессорах Intel Core, начиная с шестого поколения (Skylake), реализована технология Software Guard Extensions (SGX). Данная технология вносит новый режим выполнения кода в процессоре, режим защиты памяти, а также набор новых инструкций, которые обеспечивают работу SGX. Основная идея данной технологии заключается в создании программного анклава. Анклавы представляют собой области в памяти, заполненные зашифрованными страницами кода и данных. Расшифровка анклавов осуществляется непосредственно на центральном процессоре, после того как пройдены все проверки. Такой подход полностью защищает данные пользователей от утечки информации в открытом виде в оперативную память или в другие устройства ввода-вывода. Таким образом, какими бы привилегиями ни обладал субъект, в том числе ядра (кольцо 0),

гипервизора (кольцо "-1"), SMM (кольцо "-2") или AMT (кольцо "-3"), ему не удастся ни прочитать, ни записать страницы памяти, принадлежащие анклаву.

Применять технологию SGX в сфере облачных технологий предлагается следующим образом: пользователям предоставляются в распоряжение виртуальные машины по модели PaaS или SaaS. Для организации безопасной облачной системы требуется специально разработанный гипервизор, который будет обеспечивать создание SGX контейнеров для каждой из виртуальных машин и проверку подлинности пользователя. После этого защищенные контейнеры предоставляются конечным пользователям, которые самостоятельно решают, каким образом их использовать, и какие действия в облаке будут выполняться внутри SGX анклава. Применение такого подхода обеспечивает недоступность пользовательских данных для провайдера облачных вычислений. Ещё один из вариантов использования технологии – разработка облачного сервиса типа SaaS для хранения и обработки различных документов, а также обмена ими. Ключевой особенностью такого сервиса является использование защищенных анклавов для работы с объектами определенного типа, например, документами.

Предложенный подход к организации безопасных облачных вычислений, за счет применения технологии SGX, обеспечивает защиту конфиденциальных данных пользователей облачных систем на уровне процессора при сохранении всех преимуществ технологии облачных вычислений, что позволяет уменьшить поверхность доверия пользователя до производителя процессоров Intel.

Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПОСТРОЕНИЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Для управления устойчивым развитием предприятия необходимо сформировать соответствующую стратегию, включающую разработку системы показателей деятельности предприятия. В основе функционирования современных производственных комплексов лежит связь отдельных структурных подразделений, которые взаимодействуют между собой в рамках системы распределенного производственного комплекса, позволяющего:

- осуществлять управление процессами на основе межсетевого взаимодействия с использованием глобальных информационных сетей;
- контролировать производственный процесс и загружать программное обеспечение в производственный цикл из любой доступной точки сетевого взаимодействия;
- формировать структуру цикла с учетом загруженности предприятий, входящих в отрасль.

Одним из основных требований, выдвигаемых при внедрении технологий управления распределенным производством на современном этапе развития, является обеспечение защиты информации от случайных и злонамеренных воздействий, а также бесперебойное поступление информации к объекту управления.

Вместе с тем избыточные меры по обеспечению безопасности влекут за собой неоправданно большие, а при определённых условиях и неприемлемые расходы. В этом случае для определения оптимального набора средств защиты необходимо введение группы показателей для информационных и физических компонент производственного процесса, а также показателей, характеризующих состояние системы в целом.

При рассмотрении устойчивого функционирования как конечного состояния, возникает вопрос об измеримости и критериях определения его достижения. В этом случае необходимо в первую очередь проанализировать данные, полученные путем измерения процессов. Для этого выполняется определение пространства характеристик и метрик, спецификация процессов, протекающих при функционировании предприятия, и формирование управляющих сигналов в условиях потери устойчивости состояния.

Одним из этапов построения системы показателей безопасности предприятия является исследование и классификация статистических характеристик потоков информационных систем с использованием специальных оценочных характеристик для выявления уязвимостей и аномалий. Это позволяет построить иерархическую систему показателей безопасности, основанную на учете изменений их параметров. В этом случае можно использовать показатели, различные по масштабу охвата – показатели уровня функционирования предприятия, отдела, процесса. Процесс, в свою очередь, можно представить в виде сценария взаимодействия устройств, что позволяет обеспечить измерение показателей на конкретном устройстве.

Показатели низких уровней могут измеряться непосредственно на оборудовании, более масштабные – с помощью свёртки низкоуровневых показателей. Свёртка применяется для установления взаимосвязи показателей верхнего и нижнего уровней. Подобное деление общей схемы на подуровни позволяет осуществлять мониторинг функционирования как отдельных узлов и

подсистем, так и предприятия в целом. Систему показателей можно представить в виде иерархического дерева с корнем в вершине интегрального показателя верхнего уровня.

Применение данного подхода является относительно простым, поддается формализации и в значительной степени может быть реализовано автоматически.

Таким образом, разработанная иерархическая система показателей безопасности позволяет с требуемой степенью детализации получить количественные характеристики как устройств, так и подсистем и предприятия в целом, а также обеспечить сравнение полученных показателей. Для обеспечения безопасности и анализа состояний конечных устройств могут быть использованы программно-аппаратные модули, построенные на базе агентно-ориентированных моделей сетевого взаимодействия и методов фильтрации на основании изменения параметров представленных показателей соответствующего уровня.

Федорченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ХОСТ-ОРИЕНТИРОВАННАЯ МЕТОДИКА КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

В настоящее время проблема обеспечения кибербезопасности государственных, промышленных, военных и финансовых объектов остается актуальной. Данный факт обусловлен как нарастающей популярностью целевых атак, так и заинтересованностью злоумышленников во вредоносном воздействии на компьютерные инфраструктуры с целью получения выгоды. Данная работа посвящена разработке хост-ориентированной методики корреляции событий безопасности для использования в системах управления событиями и информацией безопасности (Security Information and Event Management, SIEM).

Для обеспечения безопасности компьютерных инфраструктур в данный момент существует большое количество средств. Одним из классов таких решений являются SIEM-системы. Основное направление работы данных систем заключается в анализе информации безопасности (в том числе событий) из различных источников, таких как: сетевой трафик, системные журналы событий, события средств защиты, статическое состояние системы и его изменения. В начале процесса обработки над данными проводятся подготовительные этапы нормализации, предобработки и анонимизации, после чего применяются специальные методы корреляции событий безопасности.

Задача корреляции событий безопасности сводится к объединению данных в более высокоуровневые структуры с целью дальнейшего выделения среди них инцидентов безопасности. Работы по данному направлению ведутся уже более 20 лет и выбор конкретных методов зависит от реализации каждого предлагаемого решения. Однако, с учетом роста объема обрабатываемых и хранимых данных, а также увеличением количества целевых атак, существующие решения являются не достаточно эффективными для обеспечения безопасности защищаемых инфраструктур.

Более ранние исследования позволили выделить преимущества и недостатки каждого из методов корреляции. Однако, наряду с выбором тех или иных методов для корреляции данных, важной задачей является порядок обработки и архитектура системы с учетом больших данных. Очевидно, что использование только одного метода не является достаточным для эффективного решения задачи корреляции. Таким образом, предлагается использовать как сигнатурные методы (правило-ориентированный подход) наряду с интеллектуальными методами (искусственные нейронные сети).

Принципиальным архитектурным решением задачи является корреляция событий как централизованно, так и на хостах (конечных сенсорах) системы так, где это возможно. Однако, принимая во внимание, что конечные сенсоры могут быть слишком различны (иметь совершенно разный формат событий и некоррелируемое содержимое), и что при построении нейронных сетей с большим количеством незадействованных входных сигналов нулевого слоя может наблюдаться потеря эффективности их применения, предлагается сегментировать защищаемую инфраструктуру по ее ключевым признакам. Частным случаем сегментирования инфраструктуры является типизация хостов.

Под данной операцией понимается разделение всех конечных сенсоров системы на определенные типы. Например, отдельным сегментом может являться определенная операционная система одного структурного подразделения объекта, с заранее известными возможностями и ограничениями обслуживающих их операторов. Также имеет смысл производить сегментирование по другим критериям, например: локальное и физическое расположение сенсоров, должности обслуживающего персонала, политика безопасности и др.

Разрабатываемая хост-ориентированная методика корреляции событий состоит из следующих основных элементов: (1) анализ связей событий типового элемента инфраструктуры; (2) выделение свойств системы, являющихся атрибутами событий (имя пользователя, адрес и др.); (3) выделение сессий внутри хоста; (4) проверка целостности событий, в рамках одной сессии; (5) построение (уточнение) модели искусственной нейронной сети с признаками целостности и принадлежности к

типовому элементу (хосту). Таким образом, перед отправкой информации и событий безопасности в центр анализа помимо предварительных этапов обработки предлагается производить корреляцию событий внутри одного хоста на основании его типа.

Рассмотренный подход корреляции событий безопасности направлен как на увеличение скорости обработки данных и поддержания системы в режиме реального времени, так и на проведение более детального анализа поступающих событий, а предполагаемый результат работы данной методики направлен на повышение эффективности SIEM-системы, в котором она будет применяться.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Хитов С.Б., Еременко С.П., Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербургский университет МВД России

К ВОПРОСУ ОБ ОЦЕНКЕ ЗАЩИЩЕННОСТИ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Современные стандарты и требования по обеспечению информационной безопасности (ИБ) предусматривают в рамках создания в организациях системы обеспечения информационной безопасности (СОИБ) проведение комплексного обследования (или аудита) состояния защищенности, как отдельных объектов информатизации, так и объединяющих их систем. Это определяет значимой и актуальной задачу оценки защищенности эксплуатируемых и внедряемых в организациях информационных систем, в том числе распределенных.

В настоящее время оценка защищенности, аттестация и сертификация информационных и автоматизированных систем производится по большей части, в соответствии с требованиями действующих в нашей стране нормативных, правовых и руководящих документов отечественных регуляторов в области ИБ, а также государственных и международных стандартов.

При этом требования по защищенности и безопасности к ИС, относящимся к классу сложных систем, носят зачастую характер требований к отдельным или к небольшим и относительно несложным системам.

Это ведет к необходимости при создании СОИБ в целях наиболее объективной оценки защищенности ИС проведение анализа, исследований, оценки и формулировки требований по защищенности и безопасности к ИС с учетом их сложности.

Таким образом, на начальном этапе построения системы защиты информации сложной ИС, в том числе распределенной, первостепенной задачей становится оценка необходимого уровня требований по защищенности и заданием градуированных по сложности классов защищенности.

Существует несколько подходов к разделению систем по сложности. На начальном уровне оценки наиболее применяется градация в зависимости от числа элементов, входящих в систему. При этом выделяют четыре класса систем :

- малые системы (10...103 элементов);
- сложные (104...107 элементов);
- ультрасложные (107. ..1030 элементов);
- суперсистемы (1030.. .10200 элементов).

Принимая во внимание подобное разделение, для построения модели ИБ предлагается следующая классификация ИС по уровню сложности:

- для сложности до 10 рабочих мест – ИС-4;
- для сложности от 10 до 100 рабочих мест – ИС-3;
- для сложности от 100 до 1000 рабочих мест – ИС-2;
- для сложности выше 1000 рабочих мест – ИС-1;

С учетом таких факторов как угрозы и риски ИБ, уязвимости ИС, для построения сбалансированной СОИБ предполагается первоначально провести анализ рисков в области ИБ. Затем определить оптимальный уровень риска ИС на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемый в модели механизм расчета оценок потребует наличия данных по вероятности атак, как на отдельные рабочие места, так и на ИС в целом.

Для компенсации увеличения числа нарушений ИБ в ИС по причине роста их сложности, предусматривается изменение требований по безопасности к системам, в сторону их увеличения с ростом класса защищенности, а также применение дополнительные защитных меры для сложных ИС соответствующих классов в привязке к перечню мер и требований, определяемых РД ФСТЭК России и ГОСТ Р ИСО/МЭК 15408-1-2012.

Хитов С.Б., Еременко С.П., Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербургский университет МВД России

НЕКОТОРЫЕ АСПЕКТЫ ОБОСНОВАНИЯ СРЕДСТВ ФИНАНСОВГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ

Ни для кого не секрет, что надежное обеспечение информационной безопасности (ИБ) в организациях требует выделения на эти цели необходимых и достаточных ресурсов, а одной из задач подразделений (служб) ИБ организаций, является задача обоснования перед высшим руководством необходимых средств финансового обеспечения (СФО) как отдельных проектов или решений, так и ИБ организации в целом.

Реализация процессного подхода к управлению ИБ предполагает выделение ресурсов как на реализацию процессов, связанных с оценкой и обработкой рисков, выявление и обеспечение требований соответствующих нормативных правовых документов в области ИБ (международных стандартов, российского законодательства, требований государственных регуляторов, договорных обязательств), так и на поддержку требований бизнеса процедурами ИБ.

Одним из ключевых моментов, оказывающих существенное влияние на процесс принятия высшим руководством организаций решений, связанных с выделением СФО ИБ, является различие в восприятии их обоснования.

Как правило, служба ИБ при обосновании СФО оперирует такими понятиями как угрозы и связанные с ними риски, а также необходимостью выполнения требований различных нормативных правовых документов. В то время как высшее руководство организаций при планировании деятельности (в том числе связанной с обеспечением ИБ) и обосновании выделения ресурсов, необходимых для ее осуществления воспринимает два основных понятия: затраты (расходы) и прибыли (выгоды). При этом, безусловно, руководство будет заинтересовано в осуществлении той деятельности (а, следовательно, и в выделении ресурсов на эту деятельность), результатом которой будет превышение прибыли над затратами.

С такой точки зрения при обосновании СФО ИБ как специалистами службы ИБ, так и высшим руководством организации отчетливо видятся и воспринимаются именно расходы на ИБ, в то время как прибыли, или выгоды получаемые организацией от реализации того или иного проекта или решения, связанного с обеспечением ИБ зачастую остаются за рамками понимания. Кроме того, определение и надлежащее предоставление подобных прибылей высшему руководству может представлять для службы ИБ довольно сложную задачу. Исключением, по мнению авторов, здесь может быть обоснование СФО на мероприятия ИБ, которые позволяют организации избежать штрафных санкций за нарушение установленных законодательством Российской Федерации (РФ), регулирующим вопросы обеспечения ИБ требований (например, обоснование в необходимых случаях СФО на применение средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства в форме обязательной сертификации).

В большинстве же остальных случаев, когда проекты или решения ИБ направлены на поддержку требований бизнеса, для обоснования СФО специалистам служб ИБ необходимо понимание бизнес-процессов, реализующихся в организации, их ключевых показателей, четкое видение места и роли, обеспечивающих данные бизнес-процессы информационных систем и ресурсов, а также задач, решаемых предлагаемым проектом ИБ.

Здесь речь может идти о тех потерях, прежде финансовых, связанных с прямым денежным ущербом, которые может понести определенный бизнес-процесс, либо несколько взаимосвязанных бизнес-процессов, а значит и в целом организация, проигнорировав реализацию предлагаемого проекта ИБ. При этом важно количественно оценить размеры подобных потерь, сопоставить их с затратами на внедрение мероприятий ИБ, показать руководству организации выгоду (прибыль) от их реализации.

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТРИЧЕСКАЯ ОЦЕНКА ФАКТОРОВ РИСКА НА ОСНОВЕ СТРУКТУРНОЙ ИНФОРМАЦИИ ПРИ КОГНИТИВНОМ ПОДХОДЕ

Анализ и, в частности, оценка рисков в последние годы по понятным причинам стали распространённым занятием — проблемы безопасности во многих областях деятельности объективно требуют пристального внимания, а информационная безопасность в них играет ключевую роль. Имеются стандартные процедуры оценивания рисков, они относительно просты для применения, что необходимо для практики, но их императивность при отсутствии достаточной теоретической обоснованности делают оценки, получаемые с их помощью, не всегда убедительными, хотя и бесспорными по определению. В то же время для сложных, слабоструктурированных и критически важных ситуаций необходим нестандартный тщательный анализ. В этом случае трудно обойтись без знаний экспертов, но без включения в формальные модели они (знания) могут быть

выражены преимущественно вербально, что допускает наличие не менее обоснованных альтернативных суждений.

Существуют разнообразные формализованные подходы, методики, способы, так или иначе, более или менее обоснованно или эвристически, без обоснования, использующие экспертные оценки факторов риска лишь для расчётов в соответствии с некоторым алгоритмом и получения искомых показателей, то есть первичной и самодостаточной становится модель, методика анализа, которая и диктует набор исходных данных.

Рассматривается гипотеза о том, что при анализе рисков для сложных не достаточно определённых объектов и ситуаций более существенной по сравнению с обычно используемыми исходными метрическими оценками является «структурная информация» о системе взаимодействующих факторах риска, представляемой причинно обусловленной структурой, что позволяет наш подход отнести к так называемому когнитивному.

В нашей методике риск-анализа, реализованной в виде автоматизированной системы, кроме структурного аспекта значительное внимание уделено также и метрическим оценкам с большим разнообразием способов их задания. За счёт процедуры гомогенизации они преобразуются в распределения случайных величин в интервале не шире (0, 1). Однако опыт применения данной методики с различным уровнем метрической наполненности модели и некоторые общие соображения в какой-то мере подтверждают справедливость высказанной гипотезы.

В самом деле, поскольку вычислительный алгоритм сводится к матричным операциям над случайными величинами, то есть к их произведениям и суммам этих произведений, также являющихся случайными величинами, возникает вопрос о свойствах результирующих показателей, если произведения длинные, а сумм много, то есть структура достаточно сложная. Аналитически в общем виде ответить на него не представляется возможным, однако нетрудно показать, исходя из выражения для дисперсии произведения независимых случайных величин, при вполне допустимом по смыслу допущении, что относительный показатель рассеяния (с.к.о., делённое на м.о.) исходных величин соразмерен у двух сомножителей, для их произведения он возрастёт почти в полтора раза. Но даже если снять допущение, то этот показатель всё равно увеличится так же, но по сравнению со среднегеометрическим показателем сомножителей, что медленнее, но всё равно будет приводить к относительному росту дисперсии по мере увеличения количества сомножителей.

Что касается сумм, то здесь возможны три варианта: суммируются произведения, полученные по непересекающимся путям графа структуры — в этом случае слагаемые будут независимы, и их дисперсии просто складываются, и два варианта, не считая их комбинации, для пересекающихся путей. Пересекаться могут дуги или вершины, и случайные произведения тогда будут зависимы, но в одном случае корреляция будет положительной, а в другом — отрицательной. На больших сильно связных структурах количество путей разного типа будет велико, и поэтому есть основания предполагать, что в итоге суммирования за счёт взаимной компенсации слагаемых последних двух типов, дисперсия будет неуклонно расти. Кроме того, получаемые промежуточные распределения с разной асимметрией будут при операциях над ними сглаживаться, и не исключено, что в пределе ограниченное интервалом (0, 1) распределение будет стремиться к равномерному, и исходная структурная информация тогда будет иметь решающее значение.

Важность предполагаемого факта определяется тем, что, во-первых, задание экспертом метрических оценок часто вызывает понятное отторжение со снижением качества результата. Во-вторых, что более важно, знания эксперта должны использоваться эффективно, то есть он должен предоставлять наиболее существенные, системные сведения, отражающие глубокое знание предмета, а не оценочные суждения. Приведённое обоснование не является доказательством, но обнадёживает. Кроме того построение структур может быть автоматизировано с применением различного инструментария, в частности, технологий больших данных, нейронных сетей, средств семантического анализа.

Юмашева Е.С., Теплов Э.П.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ИНФОРМАЦИОННЫЕ УГРОЗЫ ОРГАНИЗАЦИИ С ПОЗИЦИИ СИСТЕМНОГО АНАЛИЗА И РУССКОЙ ЛИТЕРАТУРЫ

В литературе царит разнобой в содержательной части используемого в тематике информационной безопасности понятийного аппарата. Предлагается формулировать это содержание преимущественно с опорой на русскую культуру и системную методологию.

Например, согласно В.И.Далю угроза есть нечто, угрожающее, наводящее опасность целостности, сохранности чего-то или кого-то, вызывающее страх, опасенье за свою или иную жизнь, здоровье и имущество; запугивание, обещание причинить кому–нибудь вред, зло; опасность; то, что создает опасность безопасному состоянию объекта, субъекта. С этих позиций информационная угроза есть то, что несет опасность целостности и сохранности информации, т.е. угроза хищения и

уничтожения, повреждения и блокирования использования, вытеснения и замещения иной информацией и т.п.

Безопасность, согласно В.И.Далю, отсутствие опасности, угрозы, сохранность, надежность; такое качество состояния чего-то, кого-то, которое достигается, как правило, мерами устранения опасности, угрозы, способами охранения, обороны, закрытия и обеспечения целостности кого-то, чего-то; действия, которые загодя, вовремя защищают и ограждают чего-то, кого-то, обеспечивая целостность, сохранность и отсутствие страха перед угрозами. .

В этом случае информационная безопасность есть состояние объекта, субъекта, при котором своевременно обеспечивается целостность и сохранность имеющейся у них информации, достигаемое путем реализации субъектами специального комплекса мероприятий, сведенных в систему.

Информационная безопасность организации (частного случая системы: семьи, фирмы, банка, банды, ведомства, госаппарата в целом) с системно-аналитических позиций может быть представлена сведенными в систему комплексными мероприятиями (в этом случае это типы безопасности), обеспечивающими:

I. Информационную безопасность элементов (компонент) системы (организации): целеполагания организации (безопасного и реалистичного); руководителей организации; кадрового персонала; финансовой, материально-технической и информационной (различные носители информации – от устава до технологий, ноу-хау) баз организации.

II. Информационную безопасность организации как единой организованной системы («организационная безопасность»). Речь идет об информации обеспечивающей организованность системы, соответствующих объединяющих компоненты организации взаимосвязей-взаимоотношений.

Ярмак А.В., Павленко Е.Ю., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ОЦЕНКА БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ НА ОСНОВЕ НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ

Наиболее распространенной операционной системой (ОС) для мобильных устройств является ОС Google Android. Такая популярность обусловлена открытостью данной платформы и большим количеством функциональных возможностей, заключающихся в установке приложений не только с официального магазина Google Play Store, но и с альтернативных рынков приложений. При этом, в приложениях, загруженных с альтернатвных источников, анализ безопасности может не осуществляться. Данный факт делает мобильные устройства под управлением ОС Google Android с хранящимися на них различными учетными данными, сведениями о банковских картах и личной информацией пользователя привлекательными для злоумышленников. Как правило, основными целями атакующих являются кража денег, получение контроля над устройством, финансовые выгоды от троянских коней. При этом, современные способы защиты мобильных устройств не могут с высокой вероятностью определить, является ли устанавливаемое приложение вредоносным.

Известно значительное число исследовательских работ, посвященных разработке методов анализа безопасности Android-приложений. Данные методы условно можно разделить на подходы с использованием статического анализа, когда исследование содержимого приложения производится без его реального выполнения, а также на подходы, основанные на динамическом анализе, в ходе которого информация о поведении приложения регистрируется во время его исполнения на виртуальной машине или реальном устройстве. Также, наряду с вышеперечисленными подходами, в последнее время все большей популярностью начинают пользоваться методы машинного обучения, которые показали свою эффективность применительно к задаче обнаружения вредоносного программного обеспечения.

Для решения сформулированной выше проблемы предлагается разработка системы анализа безопасности Android-приложений, основанной на методах статического и динамического анализа для сбора информации о поведении приложения и методы машинного обучения для принятия решения о том, является оно вредоносным или нет.

Принадлежность объектов к каким-либо классам целесообразно определять динамически, в процессе обучения. Однако, в процессе принятия решения о принадлежности приложения к тому или иному кластеру, может возникнуть неопределенность, когда по входному вектору, характеризующему приложение, невозможно однозначно решить, является приложение вредоносным или нет. Для решения данной проблемы предлагается использовать методы нечеткой кластеризации, позволяющие каждому объекту относиться с различной степенью принадлежности к нескольким или ко всем кластерам одновременно. Таким образом, использование методов кластеризации позволяет значительно сократить объем хранимой информации в случае большой обучающей выборки, так как для определения принадлежности объекта к кластеру понадобятся лишь наиболее типичные представители от каждого кластера – центры кластеров.

На основе данных, получаемых в результате статического и динамического анализа, можно составить описание поведения приложения, сформировав n-мерный вектор характеристик. В результате анализируемые приложения проецируются в векторное пространство с некоторой

введенной мерой близости, на основе которой и происходит разбиение объектов на кластеры и определение их наиболее типичных представителей. В процессе анализа безопасности приложения вычисляются расстояния между вектором, характеризующим данное приложение, и центрами кластеров, полученных в результате обучения модели. Из полученных значений выбирается минимальное, и на основе этого принимается решение об отнесении его к какому-либо из кластеров.

Для оценки качества кластеризации при различных мерах близости был проведен сравнительный анализ на тестовой выборке с применением следующих мер близости: евклидова расстояния, квадрата евклидова расстояния, расстояния Хэмминга и расстояния Чебышева. В качестве критериев оценки использовались индекс отделимости, индекс разбиения и индекс Хие-Бени. Результаты анализа показали, что применительно к поставленной задаче и заданному формату входных данных, наилучшее качество разбиения достигается при использовании евклидовой метрики в качестве меры близости.

В данной работе приведена экспериментальная оценка предложенной системы. Среди 1000 проанализированных приложений, из которых 403 являлись вредоносными, доля истинно распознанных образцов безопасных приложений составила 76%, доля истинно распознанных вредоносных образцов – 83%. Полученные результаты свидетельствуют о высоких показателях точности обнаружения и позволяют сделать вывод об эффективности данного подхода применительно к задаче обнаружения вредоносных Android-приложений.

ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИ

Березкина Е.Н.
Россия, Санкт-Петербург, Информационный центр Главного управления МВД РФ по г. Санкт-Петербургу и Ленинградской области

ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ ПРИНЯТИИ РЕШЕНИЯ О ВСТУПЛЕНИИ ГРАЖДАН В ОБЩЕСТВЕННЫЕ ОБЪЕДИНЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ НАПРАВЛЕННОСТИ

Полиция в современных условиях деятельности должна оказывать поддержку развитию гражданских инициатив в сфере предупреждения правонарушений и обеспечения правопорядка. Одна из форм такой поддержки – стимулирование участия граждан в охране общественного порядка.

Участие граждан в охране общественного порядка – это оказание гражданами помощи органам внутренних дел (полиции) и иным правоохранительным органам в целях защиты жизни, здоровья, чести и достоинства человека, собственности, интересов общества и государства от преступных и иных противоправных посягательств, совершаемых в общественных местах.

Для принятия решения об участии в мероприятиях подобного рода граждане должны соответствовать определённым требованиям и соблюдать ряд ограничений и запретов. Так, не могут быть приняты в состав общественных объединений правоохранительной направленности, участвующих в охране общественного порядка граждане:

- имеющие неснятую или непогашенную судимость;
- в отношении которых осуществляется уголовное преследование;
- ранее осужденные за умышленные преступления;
- страдающие психическими расстройствами, больные наркоманией или алкоголизмом;
- признанные недееспособными или ограниченно дееспособными по решению суда, вступившему в законную силу;
- подвергнутые неоднократно в течение года, предшествовавшего дню принятия в общественное объединение правоохранительной направленности, в судебном порядке административному наказанию за совершенные административные правонарушения;
- имеющие гражданство (подданство) иностранного государства.

Согласно действующему законодательству полиция имеет право обрабатывать данные о гражданах, и формировать банки данных о гражданах. В данных информационных ресурсах может быть получена следующая информация, способная охарактеризовать гражданина:

- о лицах, подозреваемых или обвиняемых в совершении преступления;
- о лицах, осужденных за совершение преступления;
- о лицах, которые совершили преступление или общественно опасное деяние и в отношении которых судом применены принудительные меры медицинского характера;
- о лицах, в отношении которых вынесено постановление о прекращении уголовного преследования за истечением срока давности, в связи с примирением сторон, вследствие акта об амнистии, в связи с деятельным раскаянием;
- о лицах, в отношении которых до вступления приговора в законную силу был применен акт помилования или акт об амнистии, освобождающие от наказания;
- о лицах, совершивших административное правонарушение;
- о лицах, объявленных в розыск;
- о лицах, находящихся в беспомощном состоянии и неспособных по состоянию здоровья или возрасту сообщить сведения о себе;
- о владельцах транспортных средств;
- о лицах, являющихся иностранными гражданами;
- о лицах, признанных больными наркоманией либо потребляющих наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, на которых судьей при назначении административного наказания возложена обязанность пройти диагностику, профилактические мероприятия, лечение от наркомании и (или) медицинскую и (или) социальную реабилитацию в связи с потреблением наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ.

Данная информация предоставляется государственным органам и их должностным лицам только в случаях по соответствующим запросам и в установленные законом сроки. Для получения характеризующих данных граждан используются информационные мощности информационных

центров органов МВД России. При получении сведений о гражданах должны соблюдаться требования о неразглашении информации, ставшей известной органам внутренних дел в результате проведения соответствующих проверочных мероприятий.

Данные проверочные действия предусмотрены ФЗ №3 «О полиции», ФЗ №44 «Об участии граждан в охране общественного порядка», другими нормативными актами.

Бойкова Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ ОСНОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ МВД РОССИИ В ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ЛИЦЕНЗИОННО-РАЗРЕШИТЕЛЬНОЙ РАБОТЫ

Информационно-вычислительная система МВД России представляет собой совокупность программных, технических, информационных, организационных средств, систем передачи данных, технологий их использования и предназначена для обеспечения информационной поддержки деятельности органов внутренних дел Российской Федерации.

Статья 11 и пункт 33 части 1 статьи 13 Федерального Закона от 07.02.2011 № 3-ФЗ «О полиции» закрепляют право на использование сотрудниками полиции в служебной деятельности достижений науки и техники, современных технологий и информационных систем, автоматизированных информационных систем, интегрированных банков данных.

В целях реализации Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел», утвержденной приказом МВД России от 06.12.2004 № 813 к настоящему времени разработана и уже функционирует единая система ЕИТКС МВД России, созданы отдельные учетные АИС по различным направлениям.

Информационное обеспечение подразделений лицензионно-разрешительной работы ОВД заключается в тщательном отборе из всей совокупности информации только тех сведений, которые необходимы и достаточны конкретному сотруднику ОВД определенного уровня для эффективной организации его работы. Эти сведения должны быть предоставлены в нужный момент и в необходимом объеме, и конечно для начала, непосредственно на его рабочее место.

ИСОД МВД включает интегрированную мультисервисную телекоммуникационную сеть (ИМТС), систему централизованной обработки данных (ЦОД) и программно-технических комплексов (ПТК), прикладные сервисы обеспечения повседневной деятельности подразделений МВД (повседневные сервисы), прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД (служебные сервисы), а также подсистему поддержки взаимодействия подразделений МВД с населением и межведомственного взаимодействия и подсистему обеспечения информационной безопасности. Использование и создание системы централизованного учета оружия (СЦУО) основано на приказе МВД России от 15.10.2014 № 883 «О системе информационного обеспечения централизованного учета оружия, контроля за соблюдением законодательства Российской Федерации в области оборота оружия, частной детективной (сыскной) и охранной деятельности Министерства внутренних дел Российской Федерации».

Система информационного обеспечения централизованного учета оружия (СЦУО), позволяет обеспечивать контроль за соблюдением законодательства Российской Федерации в области оборота оружия, частной детективной (сыскной) и охранной деятельности Министерства внутренних дел Российской Федерации. СЦУО состоит из взаимосвязанных между собой следующих подсистем: автоматизированная информационная поисковая система «Оружие-МВД», предназначенная для обеспечения деятельности подразделений лицензионно-разрешительной работы органов внутренних дел Российской Федерации по контролю за соблюдением законодательства Российской Федерации в области оборота оружия, частной детективной (сыскной) и охранной деятельности, с модулем предоставления (оказания) государственных услуг и центральный ссылочный массив СЦУО, предназначенный для консолидации и предоставления сведений о зарегистрированном МВД России оружии сотрудникам заинтересованных подразделений и учреждений системы МВД России.

Кроме использования собственных компьютерных учетов в области лицензионно-разрешительной работы сотрудник подразделения данного направления использует программно-технический комплекс «ИБД-РЕГИОН». Правовой основой использования сотрудниками подразделений лицензионно-разрешительной работы ИБД являются нормативно-правовые акты МВД России, ГУ МВД России по субъектам Российской Федерации, регламентирующие информационное обеспечение ОВД и порядок предоставления доступа к базам данных.

В соответствии с Федеральным Законом от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии» на войска национальной гвардии возлагаются задачи по федеральному государственному контролю (надзору) за соблюдением законодательства Российской Федерации в области оборота оружия и в области частной охранной деятельности, отсюда возникает вопрос о создании информационной системы учета оружия для использования в служебной деятельности сотрудников национальной гвардии, поскольку единая система информационно-аналитического обеспечения

деятельности (ИСОД) МВД России создавалась для собственного обеспечения. Однако порядок и организацию взаимодействия войск национальной гвардии и федерального органа исполнительной власти в сфере внутренних дел, в том числе и об использовании сотрудниками национальной гвардии системы информационно-аналитического обеспечения деятельности МВД России, возможно определить совместными нормативными правовыми актами, что соответствует требованиям пункта 4 статьи 9 Федерального Закона от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии».

Бурлов В.Г., Дмитриева А.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

РАЗРАБОТКА МОДЕЛИ АРМ РУКОВОДИТЕЛЯ ГРУППЫ ЭКСПЕРТОВ ОВД НА ОСНОВЕ МЕТОДА ДЕЛЬФИ

Возрастающие темпы информатизации общества повышают значение вычислительной техники в управленческих процессах руководителей подразделений ОВД. Использование возможностей современной вычислительной техники для автоматизации процесса обработки информации позволяет увеличить производительность труда, повысить эффективность работы с документами и ускорить обмен управленческой информацией. Подразделения ОВД активно используют вычислительную технику для ведения бухгалтерского учета, контроля за выполнением приказов и распоряжений, подготовки документов.

При современном уровне развития вычислительной техники и средств связи автоматизация процесса управления позволяет быстро и эффективно решать поставленные задачи, для чего создаются комплексные автоматизированные системы управления. Они включают в себя множество автоматизированных рабочих мест (АРМ) сотрудников, средства коммуникации и обмена информацией, другие средства и системы, позволяющие автоматизировать работу лиц, принимающих решения.

Создание автоматизированных рабочих мест позволяет эффективно обрабатывать большие потоки информации, которые имеют определенную структуру, зависящую от особенностей места применения. Это позволяет осуществлять индивидуальный подход к автоматизации именно тех функций, которые выполняются данным подразделением. Введение автоматизированных рабочих мест позволяет значительно сократить время выполнения работ и повысить их точность, облегчить труд сотрудников ОВД.

Руководителю подразделения ОВД необходимо постоянно принимать управленческие решения, базирующиеся на оценке мнений экспертов того или иного подразделения территориального ОВД. Проблемы построения АРМ руководителя ОВД в том, что начальник постоянно вырабатывает управленческие решения. А помощь в принятии правильного решения ему оказывает группа экспертов в конкретной узкой области, путем индивидуальных опросов, позволяющих учесть независимое мнение всех участников группы экспертов по обсуждаемому вопросу. Целью данного метода является получение согласованной информации высокой степени достоверности в процессе анонимного обмена мнениями между участниками группы экспертов для принятия решения. Известно, что использование коллективных знаний ведет к возможности нахождения сильных решений, однако в процессе обмена мнениями между экспертами может сказаться влияние авторитета коллег и все сведется к появлению популярных ответов.

Метод Дельфи позволяет разрешить это диалектическое противоречие. Для этого прямые дискуссии экспертов заменяются индивидуальными опросами. Собранные варианты ответов подвергаются статистической обработке. Полученные обобщенные ответы передаются каждому эксперту путем личного общения, либо по обычной или электронной почте с просьбой пересмотреть и уточнить свое мнение, если он сочтет необходимым. Эта процедура может повторяться несколько раз. В основу метода Дельфи положены следующие принципы:

- сформулированные в анкетах вопросы должны обеспечивать возможность выражение ответа в виде числа;
- опрос проводится в несколько туров, в ходе которых вопросы и ответы все более уточняются;
- эксперты после каждого тура знакомятся с результатами опроса;
- эксперты должны обосновывать свои оценки и суждения, отличающиеся от мнения большинства;
- статистическая обработка ответов производится последовательно от тура к туру с целью получения обобщающих характеристик.

Таким образом, с помощью метода Дельфи выявляется преобладающее суждение специалистов по какому-либо вопросу в обстановке, исключающей прямые дебаты экспертов между собой, но позволяющей им вместе с тем периодически взвешивать свои суждения с учетом ответов и доводов коллег. Пересмотр и возможность изменения своих прежних оценок на основе учета соображений каждого из экспертов и последующий анализ каждым участником совокупности причин, представленных его коллегами, стимулируют опрашиваемых к учету факторов, которые они на первых порах склонны были опустить как незначительные.

Бурлов В.Г., Павлина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ НА ТИПОВОМ ПЕРЕКРЕСТКЕ МЕГАПОЛИСА

Управление безопасностью дорожного движения (БДД) есть многогранный сложный процесс. Особыми возможностями для повышения эффективными управления безопасностью дорожного движения обладают web – технологий. Лицо, принимающее решение (ЛПР), формирует процессы обеспечения БДД в форме модели своего решения. В рамках направления использования информационных технологий для управления БДД в статье рассматривается разработка математической модели управления БДД, учитывающей возможности Web-технологий. В основу аналитической динамической модели положен закон сохранения целостности объекта. Разработка системы управления БДД на основе предлагаемой в статье модели позволит повысить оперативность управления БДД при удовлетворении требований гарантии достижения цели управления.

Современное общество нуждается в постоянном увеличении объема транспортного сообщения, повышении его надежности, безопасности и качества. Это требует увеличения затрат на улучшение инфраструктуры транспортной сети, превращения ее в гибкую, высокоуправляемую логистическую систему. При этом риск капиталовложений значительно возрастает, если не учитывать закономерности развития транспортной сети, распределение загрузки ее участков. Игнорирование этих закономерностей приводит к частому образованию транспортных пробок, перегрузке или недогрузке отдельных линий и узлов сети, повышению уровня аварийности, экологическому ущербу. Для поиска эффективных стратегий управления транспортными потоками в мегаполисе, оптимальных решений по проектированию улично-дорожной сети и организации дорожного движения необходимо учитывать широкий спектр характеристик транспортного потока, закономерности влияния внешних и внутренних факторов на динамические характеристики смешанного транспортного потока.

На сегодняшний день в России прирост числа автомашин значительно превышает строительства новых дорог. Становится очевидным, что в мегаполисах скорость движения транспортных потоков в часы пик становится минимальной, при этом повышается количество дорожно-транспортных происшествий. Благодаря развитию интернет технологий (Web-технологий) происходит автоматизация многих направлений жизнедеятельности человека, а также повышается контроль за ним, например, в соблюдении им правил дорожного движения. На основе моделей повышения эффективности управления безопасностью дорожного движения (БДД) с применением Web-технологий происходит постоянный мониторинг и отслеживание соблюдения правил дорожного движения (ПДД).

По российскому законодательству безопасность дорожного движения (БДД) - состояние данного процесса, отражающее степень защищенности его участников от дорожно-транспортных происшествий и их последствий. Обеспечение безопасности дорожного движения на типовом перекрестке мегаполиса достигается деятельностью, направленной на предупреждение причин возникновения дорожно-транспортных происшествий.

Web-технологии позволяют совершенствовать процесс управления БДД. Для этого необходимо разработать модель управления БДД, учитывающей возможности Web-технологий.

В основе деятельности, как участника движения, так и специалиста по организации и безопасности движения лежит решение человека. Человек осуществляет свою деятельность на основе модели. Поэтому для осуществления деятельности адекватной дорожной обстановки необходимо располагать правильной математической моделью решения человека. В известной литературе сложилось мнение, что построить математическую модель решения человека представляется сложным процессом. Однако без математической модели решения весьма проблематично гарантировать достижения цели управления БДД. Такая же ситуация и с построением системы обеспечения БДД, так как отсутствует критерий синтеза правильно построенной системы.

Данная совокупность факторов определяет актуальность настоящей работы. Обсуждаемая модель разрабатывается на основе закона сохранения целостности. А целью является выбор и обоснования условия гарантированного достижения цели управления БДД на основе синтеза математической модели решения управления безопасностью дорожного движения, учитывающей возможности Web-технологий.

Бурлов В.Г., Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА МОДЕЛИ АРХИТЕКТУРЫ ЭВМ, ФУНКЦИОНИРУЮЩЕЙ В УСЛОВИЯХ РАЗРУШЕНИЯ ПРОГРАММНОЙ СРЕДЫ

При использовании электронно-вычислительных машин возникает проблема обеспечения информационной безопасности. Данная проблема появляется из-за того, что всегда существуют

угрозы разрушения вычислительного процесса. Если вычислительный процесс на ЭВМ разрушается, то необходимо создать условия для того, чтобы данный процесс не разрушался.

Еще академик Анохин Петр Кузьмич отмечал в своих трудах то, что любая система характеризуется достижением положительного результата своей деятельности. В связи с этим можно допустить, что информационный процесс есть система, и, отвечая на вопрос «Каким образом мы можем сохранить условия обеспечения достижения результата?», целесообразно рассмотреть вопрос «Каким образом можно сохранить вычислительный процесс как систему?».

Из системотехники (Гуд Г.-Х., Макол Р.-Э. Системотехника. Введение в проектирование больших систем, 1954 г.) известно, что возможны только два подхода к разработке системы: на основе анализа и не основе синтеза.

Первый подход не позволяет гарантированно достигать установленной цели, а по сути лишь дает необходимое условие существования процесса. Существующие, на сегодняшний день, электронно-вычислительные машины, в различных модификациях, основаны на принципах Фон Неймана. Отличительной особенностью этой модели остается принцип единой «линейной памяти», которая адресуется последовательными номерами ячеек и в которых команды не отличимы от данных, что не позволяет гарантированно достигать цели, а это, в свою очередь, и является методологической основой создания проблем в области обеспечения информационной безопасности, а именно происходит разрушение программно-аппаратной среды тем или иным способом. Под разрушением программно-аппаратной среды следует понимать выход из строя аппаратной части и целенаправленное изменение извне, как требуемого содержания команд, так и требуемой последовательности их выполнения.

Альтернативой первому подходу является разработка архитектуры ЭВМ на основе синтеза. Разработка сложной системы на основе синтеза возможна только на основе знания закона построения функционирования системы. Отличительной особенностью данного подхода является знание такого закона. Только настоящий подход позволяет достигать поставленной цели обеспечения информационной безопасности и тем самым получать требуемый результат. Для этого следует использовать закон сохранения целостности, разработанный и реализуемый научной школой «Системная интеграция процессов государственного управления» зарегистрированный в реестре ведущих научных и научно-образовательных школ Санкт-Петербурга. Сущность этого закона определяется неразрывной связью объекта и его движения и характеризуется как взаимная трансформация свойств объекта и свойств его движения при заданном, четко фиксированном предназначении. Физически при реализации данного подхода следует выбрать определенную логическую последовательность команд, размещенных в памяти. Математически это можно осуществить только на основе алгебраических операций, связанной со свойствами несущего множества. Применяя такую алгебраическую операцию на множестве возможных состояний памяти электронно-вычислительной машины, мы можем моделировать процесс функционирования программной среды в зависимости от множества возможных пространственно-временных состояний памяти. Множество пространственно-временных состояний памяти может изменяться как из-за выхода из строя (разрушения) аппаратной части, так и из-за целенаправленного изменения извне, как содержание команд, так и последовательности их выполнения.

Наличие обратной связи является необходимым и достаточным условием построения правильной системы. Рассмотренный подход разработки модели процесса функционирования ЭВМ на основе синтеза позволил установить обратную связь в аналитической форме. Что, в свою очередь, привело к изменению программной системы в памяти ЭВМ и соответственно изменению производительности процессора как функции команд и правил их выполнения в интересах достижения цели деятельности информационного процесса, а также обеспечения информационной безопасности.

Вождаев А.В., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОВД

Информационные технологии уже давно стали неотъемлемой частью нашей жизни, глубоко проникли во все сферы общества, и нам уже сложно представить свою жизнь без гаджетов, интернета и вычислительной техники. Однако чем больше мы используем информационные технологии, тем сильнее мы от них зависим. Наличие подобной уязвимости простительно для простых граждан, но силовые структуры не могут позволить себе подобной роскоши. Таким образом, пред нами встает дилемма: повсеместное развитие информационных технологий требует, чтобы и органы правопорядка им соответствовали, с другой стороны, внедрение таких технологий глубоко в структуру управления ОВД, приводит к появлению уязвимостей иного рода, когда вся координация и система управления могут быть нарушены всего лишь одним злоумышленником, если тот сможет получить доступ в систему.

На данный момент с этой проблемой борются путем дублирования: все входящие и исходящие данные не рассматриваются в электронный форме, а переносятся на бумагу, а обмен служебной информацией ведется не только через единую сеть, а путем простых переговоров операторов по телефону. Необходимость оператора распечатывать полученную информацию, для того чтобы затем передать её на рассмотрение руководителю, и необходимость переносить имеющийся на бумаге материал в систему электронного документооборота, занимает огромное количество времени. Из-за этого, сотрудники, выполняющие эту работу, вынуждены практически безостановочно обрабатывать запросы на получение и передачу информации. Такая повышенная нагрузка, вызванная избыточностью информации, не только пагубно сказывается на личном составе, но и приводит к тому, что не все запросы могу быть рассмотрены. Ведение электронного документооборота параллельно с традиционным слишком нагружает систему, приводя к её неэффективности.

Так как система электронного документооборота уже налажена, а вскоре будет введена единая система, которая предоставит необходимый уровень защищенности, и, я надеюсь, сведет необходимость в двойном документообороте к минимуму, то, на мой взгляд, стоит использовать её, а требования по защищенности и надежности обеспечивать путем периодических проверок, когда вся, или только необходимая часть документооборота будет выводиться на бумагу, проверку этих данных будет осуществлять другое подразделение. Все данные введённые подразделение в систему будут сохраняться в центральном реестре, отвечающем за резервное копирование данных. Съем и распечатка данных из системы должны проводиться параллельно с работой данной системы, таким образом, прием и передача данных внутри системы будут проходить намного быстрее, а в реестре будут оставаться лишь последние состояния системы. Тогда, при выходе системы из строя, последние копии состояния системы будут направлены в подразделения, а затем, путем обмена информацией между подразделениями, будет достигнуто состояние системы на момент выхода из строя. Таким образом, для выхода системы из строя должна быть нарушена не только работа главного сервера, но и выведен из строя реестр, а вероятность совпадения данных событий очень мала.

Подводя итог вышенаписанному, хочется выделить следующее: на данный момент персонал, отвечающий за прием и передачу информации в ОВД, перегружен. Для того чтобы снизить нагрузку на личный состав, все действия направленные на избыточное копирование данных нужно перенести на отдельное подразделение, и ввести в работу реестры отвечающие за резервирование информации с определенного количества структурных единиц, в зависимости от технических возможностей оборудования.

Егорова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

РАЗРАБОТКА ЭЛЕМЕНТОВ СИСТЕМЫ, АВТОМАТИЗИРУЮЩЕЙ ПРОЦЕСС ОХРАНЫ КВАРТИР И КОТТЕДЖЕЙ

Сегодня вопрос безопасности стоит как нельзя более остро, растущая криминогенная ситуация заставляет владельца применять разные технические средства для организации охраны своего дома, такие как сигнализация, видеонаблюдения, система замков, способные фиксировать проникновение посторонних лиц в квартиру и своевременно подавать сигнал тревоги.

В настоящее время наиболее надежным способом охраны квартир и коттеджей является использование пультовой охраны. Автоматизация является качественно новым этапом в совершенствовании производства. В ее основу положено современное программное обеспечение, последние достижения микропроцессорной техники, а также технологии обработки сигнальных потоков от подконтрольных объектов. В процессе применения пультовой охраны объекта, передача сигналов осуществляется по нескольким каналам связи, таким как сотовая связь, обычные телефонные линии, всевозможные сети передачи данных. Основу такой охранной сигнализации составляет система, состоящая из пультов централизованного наблюдения, аппаратуры и каналов для передачи данных, объектовых подсистем и средств обнаружения (охранные или пожарные извещатели):

- датчик открывания дверей – в случае взлома двери и несанкционированного проникновения передаст сигнал тревоги;
- дымовой извещатель пожара – в случае возгорания или задымления передаст сигнал тревоги,
- датчик движения – зафиксирует движение на охраняемом объекте и передаст сигнал тревоги;
- контрольная панель – обеспечит подтверждение снятия объекта с охраны.

К средствам защиты от проникновения в дом взломщиков относятся и такие виды предупреждения, как звуки сирены или передаваемого с помощью громкоговорителя заранее записанного голосового предупреждения. Одновременно со звуковым сигналом охранная система включит и световой – например, прожекторы наружного освещения.

Подобные средства пультовой охраны обеспечивают непрерывный мониторинг охраняемых объектов, гарантируя своевременный выезд оперативной группы по тревожному сигналу. К основным преимуществам такой системы относят: надежность, оперативность, мгновенное реагирование на поступающие сигналы тревоги, сравнительно невысокая цена.

По расстоянию от объекта до средств автоматического контроля системы бывают сосредоточенного, дистанционного и телемеханического контроля.

Системы сосредоточенного контроля размещают в непосредственной близости от объекта управления.

Системы дистанционного контроля размещают на определенном расстоянии от объекта управления, они содержат специальные средства предварительной обработки для передачи контролируемых параметров по линиям связи.

Системы телемеханического контроля позволяют осуществить беспроводную связь с объектом управления.

Основной задачей системы автоматического контроля является измерение параметров объекта управления и сравнения текущих значений с допустимыми, регистрация значений параметров и их текущих отклонений от заданных, сигнализация возникновения нештатных ситуаций.

В последние годы охранные функции надежно выполняют видеоустройства, дающие возможность в любой момент получить информацию об окружающей обстановке.

Самым простым, но очень полезным и удобным устройством является видеодомофон, оснащенный видеоглазком. Система состоит из следующих главных элементов:

- наружная панель для вызова, с видеокамерой;
- квартирная панель с монитором;
- замок (электромагнитный или электромеханический).

Камера видеодомофона может передавать изображение, как на экран специального небольшого монитора, так и на экран работающего в этот момент телевизора.

Для большего удобства многие беспроводные модели предоставляют возможность удаленного управления работой оборудования с помощью мобильных устройств (смартфонов или планшетов). С их помощью можно оповестить хозяев квартир и коттеджей о появлении посторонних возле двери, прибытии гостей, видеонаблюдении за ними и начале общения с посетителями.

Ефимова А.Б.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

ПОДГОТОВКА ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА ВОЕННЫХ ИНСТИТУТОВ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ К ПРИМЕНЕНИЮ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Эффективность использования новых информационных технологий в различных областях человеческой деятельности научно доказывалась на протяжении последних 15-20 лет. Предметом научных исследований в области педагогических наук являлись вопросы, касающиеся применения НИТ в учебном процессе различных учебных заведений, в том числе и военных институтах, как по отдельным изучаемым дисциплинам, так и в образовании в целом.

Практически в каждом из исследований рассматриваются сущность и значение применения НИТ в той или иной сфере деятельности. Предполагается, что военному преподавателю достаточно внедрить результаты данных исследований, чтобы совершенствовать или повысить эффективность какой-либо рассматриваемой проблемы. Общими основополагающими всех исследований являлись основания, что военный преподаватель уже владеет определенными знаниями, умениями и навыками в области новых информационных технологий. Но может ли и готов ли сам военный преподаватель (в том числе с большим стажем работы) применять НИТ на практике?

Традиционные подходы к обучению и стремительно развивающиеся новые информационные технологии порождают противоречия между требованиями системы образования в условиях НИТ и готовностью преподавательского состава применять новые информационные технологии в своей деятельности. Военный преподаватель наряду с фундаментальной профильной (специальной) подготовкой должен иметь высокий уровень педагогического мастерства, что включает и необходимую информационную культуру, а также готовность в педагогической деятельности применять новые информационные технологии.

На практике в военных институтах войск национальной гвардии основополагающие дисциплины ведут специалисты, хорошо знающие свое дело, но традиционно применяющие модель репродуктивно-сообщающего обучения. Таким образом, возникла необходимость создания в военных институтах войск национальной гвардии единого подхода к подготовке профессорско-преподавательского состава применению новых информационных технологий.

Актуальность данной темы обуславливают несколько взаимозависимых оснований, связанных с реформированием военного образования, в частности с повышением уровня профессионального мастерства военных преподавателей в области новых информационных технологий.

Одним из оснований является задача по служебно-боевой деятельности войск национальной гвардии – это совершенствование боевой и мобилизационной готовности, боевой выучки войск, системы управления войсками на основе внедрения новых информационных технологий.

Другим не менее важным основанием актуальности темы является переход компьютеризации к информатизации военного образования с внедрением новых информационных технологий в образовательный процесс. Основная роль в этом процессе принадлежит профессорско-преподавательскому составу военных институтов войск национальной гвардии. Именно знания и навыки преподавателей по применению НИТ являются определяющим фактором их эффективного использования в образовании.

Процесс развития информационных технологий и их использование в образовании не стоит на месте. Каждый год появляются новые информационные технологии, требующие к себе новых знаний и навыков применения. Поэтому введение единичных занятий или даже краткосрочных курсов по изучению и применению НИТ не смогут повлиять на эффективность использования НИТ в образовании. Здесь требуется рассматривать подготовку применения НИТ как систематический процесс совершенствования профессионального мастерства.

В этой связи необходимо рассмотреть систему подготовки преподавательского состава военных институтов войск национальной гвардии к применению НИТ в едином разрезе с общей системой профессиональной подготовки и выработать практические рекомендации по ее организации. Для решения этой задачи представляется необходимым определить факторы, влияющие на процесс формирования готовности преподавательского состава к применению НИТ в практической деятельности, а также обосновать оптимальные подходы и направления к внедрению подготовки преподавательского состава военных институтов войск национальной гвардии применению новых информационных технологий с целью определения их роли и места в системе профессионально-педагогической подготовки.

В целом, это будет способствовать не только формированию у профессорско-преподавательского состава военных институтов войск национальной гвардии умений и навыков использования НИТ в практической деятельности, но и интенсификации учебного процесса, а также эффективности образовательного процесса в целом.

Зайцева Е.А., Ланг Т.Е.
Россия, Санкт-Петербург, Санкт-Петербургский институт внутренних войск МВД России, Санкт-Петербургский университет МВД России

МЕТОДЫ СБОРА ИНФОРМАЦИИ О ГРАЖДАНАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

С развитием в Российской Федерации информационных и коммуникационных технологий изменяется структура и динамика общественного развития, увеличивается их интеграция в правовое поле государства и общества. Наиболее значимые результаты развития этих процессов находят отражение в сфере информационного контента о персональных данных граждан.

Исходя из вышеизложенного, регулирование современных общественных отношений в информационной сфере, становятся одной из наиболее актуальных задач современного законодательства и права в области персонализации данных. Наиболее распространенными являются доступ к информационным ресурсам и использование информационных услуг, в том числе, по сбору информации о гражданах.

Основным нормативно-правовым актом, регулирующим информационную среду граждан, является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в редакции 2016 года), целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

По мнению Кучеренко А.В., указанная формулировка не раскрывает тот объем ожиданий, который возлагался обществом на принятие и последующую реализацию норм закона. Следует особенно подчеркнуть тот факт, что, придавая тем или иным сведениям конфиденциальный характер, как государство – субъект, определяющий меры к обеспечению конфиденциальности, - так и сам субъект данных преследуют конкретные цели, значительно выходящие за формулировку «защита прав и свобод».

Правовые нормы тесно связывают право на жизнь человека, его достоинство и честь. Защита частной жизни граждан Российской Федерации нашла свое отражение в Конституции РФ, Уголовном Кодексе РФ, Гражданском Кодексе РФ, Федеральном законе «Об информации, информатизации и защите информации», Законе Российской Федерации «О средствах массовой информации». Таким образом, Российская Конституция защищает право на частную жизнь. Закон гарантирует судебную защиту этого права.

Методологической основой служат различные методы познавательной деятельности: формально-юридический метод, анализ, синтез и логический метод, сравнительный и системный методы. Важным в данном направлении являются синтез и системный метод исследования, которые используются для выявления взаимосвязи различных отношений и выработки предложений по разрешению правовых проблем. Это теоретические подходы. В практике методы сбора информации о человеке очень широкие, начиная от незаконных по типу атаки его компьютера вредоносными вирусами для шпионажа, перехвата трафика или «втирания» в доверие. Но зачастую необходимости в этом нет, и пользуясь методами обычного социального инжиниринга можно разузнать очень много.

Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ четко трактует основные понятия, являющиеся основополагающими в сборе информации о гражданах, среди которых: персональные данные, оператор, обработка персональных данных.

Персональные данные пользователи вводят на различных интернет-серверах ежедневно. Существует ошибочное мнение, что это понятие означает информацию, которая содержится в паспорте и других важных документах. В действительности персональными данными являются различные сведения о человеке. Это не обязательно может быть номер или серия паспорта. Такими данными являются имя, фамилия, дата рождения, адрес электронной почты.

Оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В данном случае, расплывчатость формулировки фактически ставит в зависимость субъекта персональных данных от честности и добросовестности действий оператора, а также, от верности трактовки им законодательных норм.

Таким образом, правовые нормы о защите персональных данных рассматриваются в контексте права на неприкосновенность частной жизни. Именно поэтому, в связи с развитием информационного пространства общества, для которого характерно широкое использование информационных технологий, активный сбор и обработка информации, в том числе информации о личности, информация персонального характера должна иметь надлежащий уровень не только организационно-технической, но и правовой защиты.

Зайцева Е.А., Попова А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ

Повышение качества информационного сопровождения повседневной и оперативно-служебной деятельности должностных лиц органов внутренних дел Российской Федерации за счёт развития существующих и внедрения новых технических решений с использованием современных информационных технологий – одна из важнейших задач.

Уже не раз информация о делах государственных служащих становилась предметом атак хакеров. А происходит всё из-за неблагонадёжности мессенджеров и социальных сетей, где часто в переписках военных, полицейских, чиновников обсуждаются служебные сведения. Любую страницу в социальных сетях даже самый заурядный хакер способен взломать. Под угрозой уже не только частная, но и служебная информация. Нельзя также не учитывать тот факт, что большинство приложений, типа WhatsApp и Viber, в которых происходила утечка, являются иностранными, в то время как в России существуют свои аналоги.

Особый резонанс в общественности вызвали новости о том, что разведка США до максимума усилила шпионаж за Россией, что говорит о росте международной киберпреступности. Не трудно догадаться, что особую ценность будут представлять сведения государственных служащих.

Сегодня, защита статей и документов, в частности правительственных, внутренних дел, военных – это одна из основных проблем, стоящих перед ведомствами. В последнее время вопрос относительно того, как обеспечивается защита служебных сведений, начал беспокоить и сотрудников министерства внутренних дел России.

Обеспечить эту защиту следует как правовыми, так и организационными методами.

Организационные методы состоят в том, чтобы перевести личный состав на использование Системы информационно-аналитического обеспечения деятельности МВД (ИСОД), созданной на интегрированной мультисервисной телекоммуникационной системе (ИМТС).

Особо эффективно будет использование сервиса электронного документооборота. Его предназначение – автоматизация деятельности сотрудников органов внутренних дел.

Важно выполнить необходимый ряд задач для достижения поставленной цели, а именно: создать единое информационное пространство документационного обеспечения, оптимизировать потоки документов, повысить уровень информационной поддержки и конечно же обеспечить

безопасное хранение и разграничение доступа к информации, включая журналирование действий пользователей и электронную подпись.

Не менее полезным сервисом послужит сервис электронной почты МВД России, необходимый для автоматизации процессов обмена электронными сообщениями, образующимися в ходе деятельности сотрудников органов внутренних дел.

Существенный плюс этих сервисов в том, что доступ пользователей может быть выполнен только с тех компьютеров, которые подключены к ИМТС.

Говоря о правовой защите, стоит сказать, что она заключается в издании положений и правил, регулирующих организацию и порядок использования сервисов ИСОД. Кроме того, следует ограничить передачу служебной информации через негосударственные почтовые серверы.

Реализация данной политики, а конкретно выполнение мероприятий по обеспечению доступа подразделений университета к сервисам ИСОД МВД России, приведёт к единообразию работы со служебными документами, к большей её защищённости, а также к повышению уровня дисциплины сотрудников.

Правильная постановка вопроса о реализации комплекса мер по обеспечению сведений, составляющих служебную тайну, требует очень точной координации оперативно-служебной деятельности различных подразделений МВД между собой для достижения основной цели – обеспечения безусловной сохранности сведений от противоправного распространения.

Зингачева Д.А., Чудаков О.Е., Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

РАЗРАБОТКА ИНТЕРАКТИВНОГО ПРАКТИЧЕСКОГО ЗАНЯТИЯ ПО ДИСЦИПЛИНЕ «ПРОГРАММИРОВАНИЕ»

В настоящее время внедрение интерактивных форм обучения является одним из важнейших направлений совершенствования подготовки курсантов. Использование активных подходов является наиболее эффективным путем, способствующим их обучению. В этой связи работа, направленная на разработку интерактивного практического занятия на примере дисциплины «Программирование» по направлению подготовки 09.03.02 – Информационные системы и технологии представляется актуальной.

Основные методические инновации связаны сегодня с применением интерактивных методов обучения. Современный подход к обучению должен ориентировать на внесение в процесс обучения новизны, обусловленной особенностями динамики развития жизни и деятельности, спецификой различных технологий обучения и потребностями личности, общества и государства в выработке у обучаемых социально полезных знаний, убеждений, черт и качеств характера, отношений и опыта поведения.

Преподаватель при такой форме обучения показывает не только свою компетентность и эрудицию, но и умеет увлечь студентов новыми формами учебно-познавательной деятельности. Для этого организуются индивидуальная, парная и групповая работа, используется проектная деятельность, проводятся ролевые игры, осуществляется работа с документами и различными источниками информации. Преподаватель создает такую среду образовательного общения, которая будет способствовать деловому взаимодействию участников при взаимной оценке и контроле. В то же время, использование интерактивных форм обучения предъявляет более высокие требования к уровню подготовки преподавателя и его квалификации, который должен уже не только владеть традиционными методиками преподавания, но и уметь модернизировать их в соответствии со спецификой обучаемых, используя современные достижения науки и техники.

Учебный процесс с применением активных и интерактивных методов, в отличие от традиционных занятий, где курсант является пассивным слушателем, строится на основе включенности в него всех курсантов группы без исключения, причем каждый из них вносит свой индивидуальный вклад в решение поставленной задачи с помощью активного обмена знаниями, идеями, способами деятельности. К сожалению, на сегодняшний день не существует четкого разграничения между активными и интерактивными методами обучения, одни и те же виды методов относят как к активным, так и к интерактивным, поэтому нет и четкой классификации интерактивных методов обучения.

Обучение с использованием интерактивных форм приносит курсантам лучшие результаты: обеспечивает вовлеченность обучающихся (участие в процессе обучения активное, а не пассивное); основано на опыте; отвечает первоочередным потребностям и опирается на личные побудительные мотивы: осуществляет обратную связь; демонстрирует уважение к обучающимся; создает дружелюбную атмосферу и т.д.

Интерактивное обучение позволяет решать одновременно несколько задач, главной их которых является развитие коммуникативных умений и навыков, помогает установлению эмоциональных контактов между учащимися, обеспечивает воспитательную задачу, поскольку приучает работать в команде, прислушиваться к мнению своих товарищей. Использование интерактивных форм в

процессе обучения, как показывает практика, снимает нервную нагрузку обучающихся, дает возможность менять формы их деятельности, переключать внимание на узловые вопросы темы занятий.

Таким образом, использование интерактивной формы обучения в учебных заведениях является очень важной составляющей. Она способствует не только эффективному изучению различных вопросов, но и развитию личностных качеств курсантов, улучшению их взаимоотношений.

Целью данного исследования является выявление наиболее эффективных форм интерактивного обучения, способствующих активизации учебно-познавательных действий курсантов.

При проведении исследования решались следующие задачи:

1. Изучение форм интерактивных методов обучения.

2. Изучение методических материалов по преподаванию дисциплины «Программирование».

3.Разработка методических рекомендаций по проведению занятий по дисциплине «Программирование» с применением интерактивных методов.

Практическая значимость работы заключается в возможности использования разработанных методических рекомендаций на практических занятиях по дисциплине «Программирование» в Санкт-Петербургском университете МВД России.

Иванов А.Ю., Редковников В.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

РАЗРАБОТКА АРМ ПРЕПОДАВАТЕЛЯ КАФЕДРЫ СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ

В настоящее время, характеризующееся активным использованием информационных технологий во всех сферах жизни, наблюдается изменение процесса обучения: наряду с обычным лекционным материалом преподавателю необходимо подготовить презентации, подобрать видео и звуковые материалы, а также организовать практические занятия таким образом, чтобы в ходе их проведения обучающиеся могли работать с различными интерактивными средствами обучения (электронные учебники, интерактивные доски, обучающие программное обеспечение и т.п.).

Подготовка занятий на таком уровне представляет собой сложную задачу, так как преподавателю необходимо одновременно решить ряд задач:

- подготовка лекционного материала в электронном и в печатном виде;
- подготовка презентации на основе лекционного материала;
- подбор соответствующего аудио- и видеоматериалов, необходимых для повышения наглядности занятий;
- подготовка учебных материалов, которые можно будет демонстрировать с использованием интерактивного обучающего оборудования.

Одним из направлений решения комплекса перечисленных задач является создание специально подготовленных автоматизированных рабочих мест (АРМ) преподавателей.

АРМ преподавателя представляет собой аппаратно-программный комплекс, состоящий из компьютера, периферийных устройств и специального программного обеспечения, которое в значительной мере упростит работу по подготовке учебных занятий.

Персональный компьютер должен иметь характеристики, позволяющие в полном объёме выполнить подготовку лекций, презентаций, аудио- и видеоматериалов, пригодных к использованию на интерактивном оборудовании.

Периферийные устройства могут быть представлены клавиатурой, компьютерной мышью, монитором и звуковыми колонками (головными телефонами).

В перечень необходимого программного обеспечения рекомендуется включить Microsoft Word, Microsoft PowerPoint, Adobe Audition, Adobe Premiere.

При этом необходимым условием успешной работы с данным комплексом является наличие высокоскоростного подключения к сети Интернет.

Предлагаемый комплекс позволит обеспечить выполнение следующих функций.

1. Хранение, своевременное обновление и ознакомления преподавателей с материалами, относящимися к учебно-методической, научно-исследовательской и воспитательной работе кафедры.

2. Подготовку, изменение и хранение необходимых преподавателю отчетных документов.

3. Создание, изменение, подготовку к использованию и хранение учебных материалов по различным дисциплинам.

4. Создание, изменение и хранение данных об успеваемости обучающихся, а также статистику прохождения ими рубежного и итогового контроля.

В итоге предлагаемый комплекс упростит процесс подготовки учебных материалов и повысит его оперативность при условии сохранения высокого качества обучения.

При этом использование АРМ преподавателя, как единого аппаратно-программного комплекса, позволит в полной мере реализовать возможности современных информационных технологий в учебном процессе высшей школы.

Иванов А.Г., Куватов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

РАЗРАБОТКА ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ОФИЦЕРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ МВД РФ

В настоящее время в системе МВД уделяется большое внимание процессам автоматизации.

В связи с этим разработка элементов автоматизированного рабочего места офицера безопасности информации объекта ВТ МВД РФ является актуальной для упрощения его деятельности.

Процесс обеспечения безопасности объекта ВТ МВД РФ основан на разработке и на создании АРМ личного состава ОВД.

АРМ подразделений ОВД по обеспечению информационной безопасности имеет следующие базовые элементы:

- компьютер (ЭВМ);
- периферийные устройства (ПУ);
- оператор;
- комплекс программ для обработки информации;
- гипертекстовая система документации для пользователя;
- система подсказок;
- специальная эргономическая мебель для пользователей АРМ;
- система контроля ошибок.

Для обеспечения требуемого уровня информационной безопасности АРМ должен обеспечивать распознание и нейтрализацию проблемы, возникшей перед администратором безопасности.

Одним из основных элементов является модель, ее алгоритмическое обеспечение и программная реализация.

При рассмотрении АРМа перед лицом, принимающим решение стоит три основных задачи:

- механизм формирования угроз;
- идентификация проблемы угрозы (решение проблемы сводится к тестированию);
- устранение проблемы.

Так как элементы АРМа формируются на основе связи этих трех базовых процессов, то разработана модель, которая связывает данные три задачи с администратором безопасности.

Кадулин В.Е.
Россия, г. Москва, Московский университет МВД России

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Многие специалисты в области информационных технологий считают, что наиболее прогрессивный принцип создания информационных систем – это применение облачных технологий.

Преимущества электронного документооборота неоспоримы и состоят в том, что в результате его внедрения все структуры организации смогут функционировать в едином информационном пространстве, обеспечивающем существенное увеличение скорости обработки различных типов документов.

Министерство внутренних дел также намерено использовать в своей работе облачные сервисы (удаленные базы данных) и расширять спектр услуг, предоставляемых в электронном виде. Облачные технологии позволяют упростить доступ к удаленным сервисам, что позволяет не только повысить эффективность функционирования информационных систем, построенных на основе баз данных, но и сократить расходы на приобретение современных продуктов информационных технологий.

Существующие статистические данные показывают, что объем рынка облачных технологий в России к 2016 году может составить свыше 5 млрд. долларов. При этом если Государственная Дума примет «Закон об облачных технологиях», проект которого в настоящее время разрабатывается специалистами из Министерства связи и коммуникаций РФ при поддержке Ассоциации Облачных Технологий, экспертов из МВД, ФСБ и компаний-поставщиков облачных услуг, то огромное количество баз данных и программ, которые находятся в системе МВД - одна из проблем, которая осложняет работу министерства, – может быть переведено на новую технологическую базу.

Как отмечают эксперты из МВД и ФСБ России, если облачные технологии будут юридически лицензированы, а поставщики облачных услуг будут находиться в российском правовом поле, то с точки зрения безопасности эти технологии будут даже надежнее существующих. При государственной юридической легализации облачных технологий, ими готовы пользоваться многие российские организации – Сбербанк России, Росатом и другие.

По заявлениям руководства МВД, принято решение активно внедрять облачные технологии, которые позволит без исключения всем пользователям органов внутренних дел быть участниками

информационного процесса в зависимости от допуска и необходимости. Для повышения эффективности работы МВД планируется создание центра обработки данных, который позволит подключить все подразделения к оптоволоконным сетям, что обеспечит высокоскоростной доступ в Интернет и сделает работу сотрудников более качественной и оперативной. Особое внимание уделяется переходу на оказание госуслуг в электронном виде - именно эта сфера работы любого ведомства имеет приоритетное значение для граждан.

При внедрении облачных услуг требуется надежная аутентификация пользователей. Даже при использовании двухфакторной аутентификации или еще более высоких её уровней при каждом сеансе работы должны соблюдаться определенные протоколы и правила. Необходимо часто менять пароли, а сами они должны быть более сложными, чем в обычной практике.

Одновременно, учитывая постоянное совершенствование хакерских методов, традиционная онлайновая аутентификация для доступа к облачным системам зачастую оказывается недостаточной – особенно для систем со строго конфиденциальными данными, используемых в таких уязвимых отраслях, как финансовые системы, предприятия оборонной промышленности, здравоохранение и торговля, а также в государственных структурах. Учитывая, что интерес к облачным информационным сервисам растет в различных сферах деятельности, то необходимы новые подходы к обеспечению информационной безопасности.

Для построения надежной системы безопасности облачного сервиса необходимо соблюдать следующие правила:

1) использовать криптографические средства обеспечения сохранности данных;

2) процесс обмена информацией клиент-сервер должен быть безопасным, то есть необходимо использовать защищенные протоколы передачи данных как для доступа к серверу, так и при хранении информации и доступе к информационным ресурсам.

Таким образом, в интересах обеспечения информационной безопасности облачных технологий необходимо осваивать новые методы и средства защиты информации, учитывать инциденты, разрабатывать новые стандарты информационной безопасности, решать вопросы юридического характера. Кроме того, должна быть разработана и внедрена эффективная система мониторинга безопасности облачных технологий применительно к правоохранительной сфере деятельности.

Колесов Д.А., Куватов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

РАЗРАБОТКА ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА РУКОВОДИТЕЛЯ ПОДРАЗДЕЛЕНИЯ ОВД

Компьютерные технологии весьма облегчили жизнь современного человека. С помощью них люди решают огромное количество проблем, связанных с информационной деятельностью. В настоящее время очень трудно найти предприятия, которое не использует информационные ресурсы. Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы и т.д., проводимой органами внутренних дел. В свою очередь, результаты этой работы зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации, именно эти функции и призваны обеспечить система информационного обеспечения органов внутренних дел, которая поддерживает в настоящее время значительный объем информации.

Для автоматизации рабочего места, мною был выбран отдел кадров. Кадровые службы, являются одной из важнейших структур управления, обеспечивает укомплектование организаций, рабочими, специалистами, служащими, организацию подготовки, переподготовки повышения квалификации работников, аттестацию работников и руководителей, реализует меры, направленные на укрепление трудовой дисциплины, сокращение текучести кадров, осуществляет подготовку распорядительных документов по личному составу, необходимой статистической отчетности по кадрам, ведут в установленном порядке учет работников, в том числе военнообязанных, кадровое делопроизводство, оформляет документы для назначения работникам пенсий, решают иные вопросы, входящие в их компетенцию.

Автоматизированное рабочее место (АРМ) разрабатывается как комбинация процедур. Все процедуры оформляются в виде программных модулей, увязанных между собой функциональной зависимостью.

Проектируемый АРМ должен быть реализован в виде модулей. АРМ должен: обеспечить максимально наглядное и доступное представление входной и выходной информации; осуществлять проверку корректности входных данных. Необходимо предусмотреть возможность расширения и совершенствования программного комплекса, возможность удовлетворения изменившихся требований, не предусмотренных при проектировании. Обеспечить удобство работы пользователя, а именно: пользовательский интерфейс должен быть интуитивно понятным, должны обеспечиваться различные уровни доступа к функциям. Ввод исходных данных осуществляется пользователем путем

набора с клавиатуры в диалоговом режиме. Разработанное автоматизированное рабочее место работника позволяет быстро и эффективно производить учет работников. Избавляет от рутинных работ, связанных с заполнением данных работника в различные книги регистраций. Система проста в эксплуатации, удобна, не требует особых знаний от пользователя в области программирования и теории баз данных. Разработаны система помощи и руководство пользователю.

Созданный для использования в отделе кадров, программно-методический комплекс, позволит:

- повысить производительность труда;
- экономить время;
- автоматизировать процесс учета кадров;
- формирование и ведение базы работников;
- сократить время на формирование отчетов;
- хранить информацию в безбумажном виде.

Система предусматривает дальнейшее совершенствование. Пути совершенствования и развития системы создание новых модулей для учета кадров.

Использование ЭВМ для учета кадров оправдывает себя. Поэтому разработанная система предоставляет большие возможности в этом направлении.

Автоматизированный процесс учета кадров используется во многих коммерческих и государственных структурах.

Куватов В.И., Потехин В.С., Чудаков О.Е.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ИТ), ОБЕСПЕЧИВАЮЩИХ АВТОМАТИЗАЦИЮ ПРОЦЕССОВ ПОИСКА УГНАННЫХ АВТОТРАНСПОРТНЫХ СРЕДСТВ

Существующие средства решения задачи поиска по горячим следам в рамках плана «Перехват» угнанных транспортных средств далеко не всегда дают положительный результат за приемлемое время. Поэтому поиск новых путей или совершенствование существующих ИТ является актуальным.

Существующие в настоящее время ИТ, реализуемые на базе фоторадарных комплексов Крис «С» и Арена «С», а также комплексов видеофиксации «Каскад» и «Поток», обеспечивают:

- сбор видеоданных о транспортных потоках с сохранением их и возможностью последующего просмотра содержания видеозаписей. Однако при большом числе камер требуется значительное время для неавтоматизированного визуального анализа, что не позволяет решать задачу плана «Перехват» за приемлемые сроки;
- в ГИБДД накоплен определенный опыт автоматизированной обработки видеоизображений на основе цифровых технологий (фоторадарные комплексы Крис «С» и Арена «С», комплексы видеофиксации «Каскад» и «Поток»). Обработка данных в этих комплексах осуществляется довольно быстро (в реальном масштабе времени). Однако этот опыт касается только тех транспортных средств, которые нарушили правила дорожного движения (ПДД), да и площадь накрытия такими средствами незначительна (например, для стационарного фоторадарного комплекса Крис «С» это 1,5 - 2 км километров). Сбор сведений о нарушениях ПДД может осуществлять на центральном посту комплекса не более чем от 8 источников информации, что неприемлемо для больших городов.

Иначе говоря, упомянутые комплексы, имея элементы, которые могут оказаться полезными при автоматизации процесса поиска угнанных автомобилей, в целом, не способны решить всю номенклатуру требуемых подзадач, в частности:

- сбор данных накапливается лишь о транспортных средствах, нарушивших правила дорожного движения (для решения задачи «План перехват» требуется накопление данных в единой интегрированной базе о всех транспортных средствах в зоне рубежа контроля);
- автоматизированный сбор данных осуществляется до уровня центрального поста, а необходимо обобщение данных за весь запланированный район поиска, т.е. многих постов (в большом городе их могут быть сотни и даже тысячи).

В этой связи возникает потребность расширения возможностей существующих ИТ и повышения степени их интеграции. В этом и заключается новизна предлагаемого подхода.

В качестве возможных направлений совершенствования существующих ИТ (для поиска угнанных автомобилей) предлагаются следующие:

- обеспечение цифровой обработки данных не только о нарушителях ПДД, но и данных о всех транспортных средствах пересекающих рубеж контроля. При этом, в уже развернутых комплексах должен быть проработан вопрос лишь о модернизации программного обеспечения с максимально возможным сохранением имеющегося оборудования;
- создание интегрированной база данных (ИБД), объединяющей сведения, поступающие от всех центральных постов систем видеонаблюдения (района, города и пр.);

– создание (модернизация имеющихся) автоматизированных рабочих мест (АРМов): дежурной части (АРМ-ДЧ), группы оперативного управления (АРМ-ГОУ) и дежурного (АРМ-Д). При этом существующее программное обеспечение АРМов должно быть расширено средствами, обеспечивающими:

– учет данных о краже (угоне, использовании в преступлении) транспортного средства; в объеме, предусмотренном соответствующими руководящими документами;

– обеспечения документируемой возможности принятия решения о введении плана «Перехват» должностными лицами, имеющими соответствующие полномочия;

– обеспечение визуализации результатов поиска с отображением информации на фоне карты города (района, зоны поиска);

– объединение АРМов и ИБД локальной городской или районной вычислительной сетью с максимальным использованием возможностей существующей единой ведомственной информационно-телекоммуникационной сети МВД (ЕИТКС).

Совокупность упомянутых АРМов, ИБД и телекоммуникационных средств можно рассматривать в качестве элементов автоматизированной системы выполнения плана «Перехват» (АСПП). Реализация такой АСПП должна радикально изменить ситуацию с перехватом транспортных средств после объявления их в розыск.

Куватов В.И., Синещук Ю.И., Синещук М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России

ПРОБЛЕМА ВЫБОРА РАЦИОНАЛЬНОГО СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Научно-технический прогресс, создание и глобальное распространение электронных технологий, особенно сети Интернет, стало основной причиной появления и распространения киберугроз. Кибербезопасность сегодня рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества.

Для предотвращения кибератак, реализующих соответствующие киберугрозы создаются системы защиты информации (СЗИ), сужающие область киберуязвимостей современных инфоромационных систем. СЗИ, в общем случае, состоят из ряда подсистем, в основе которых лежат комплексы организационных, законодательных, физических, аппаратных, программных, инженерно-технических, морально-этических методов и средств.

Работа по созданию СЗИ состоит из нескольких этапов:

– подготовительный этап;
– инвентаризация информационных ресурсов;
– анализ рисков;
– составление плана работ по созданию СЗИ;
– реализация плана работ по созданию СЗИ.

Один раз созданная СЗИ не будет оставаться хорошей всегда. Неизбежно подойдет время, когда возникнет необходимость в модернизации или замене СЗИ.

Основная трудность в работе по созданию СЗИ, по управлению информационной безопасностью связана именно с выбором методов и средств защиты информации, и требует точной количественной оценки защищенности информационных ресурсов. Для количественной оценки эффективности СЗИ наибольшее применение находят модели, в основе которых лежат методы математического программирования и методы теории игр.

Методы математического программирования целесообразно применять в тех случаях, когда множество потенциальных нарушителей размыто. В том случае, когда известен круг лиц, регулярно осуществляющих попытки НСД к информационным базам, более точными оказываются игровые модели.

Разработка модели на базе методов математического программирования начинается с уяснения того, что и от чего нужно защищать. Для ответа на данные вопросы выявляется перечень защищаемых ресурсов и перечень возможных угроз каждому из защищаемых ресурсов. Затем оценивается интенсивность возникновения возможных угроз и величина ущерба от их реализации. После этого определяется перечень методов и средств, с помощью которых может быть нейтрализована каждая из этих угроз, вероятность нейтрализации каждой из возможных угроз каждым из возможных методов и средств.

Следующим этапом математического моделирования является этап разработки критерия эффективности СЗИ. Критерий эффективности должен соответствовать назначению моделируемой СЗИ и иметь ясный физический смысл. Кроме того, критерий эффективности в качестве своих переменных должен содержать перечень и количество возможных методов и средств СЗИ (должен быть чувствительным к характеристикам методов и средств, которые могут быть включены в состав СЗИ).

На заключительном этапе разработки математической модели необходимо установить ограничения на количество методов и средств СЗИ.

В игровых моделях сторона, защищающая свои информационные базы, называется первой стороной, а нарушители – второй. Первая сторона строит СЗИ, а вторая – преодолевает ее. Затем первая сторона строит новую СЗИ и т.д. Если вторая сторона преодолела СЗИ раньше того времени, когда первая построила новую – первая сторона проиграла. В этих моделях критерием эффективности является функция двух аргументов: времени первой стороны затрачиваемого на построение СЗИ и времени второй стороны на ее преодоление. В более сложных моделях рассматривается не только время, но и стоимость защищаемой информации и затраты на преодоление защиты.

Для потенциально-опасных, критически важных информационных систем наиболее характерной является ситуация, при которой можно говорить о потенциальных нарушителях. При этом перечень потенциальных нарушителей достаточно обширен и нечеток. Поэтому при создании СЗИ таких объектов большее применение находят модели, основанные на методах математического программирования.

Куватов В.И., Скрипниченко А.Ю., Санкт-Петербургский университет МВД России

РАЗРАБОТКА СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ОТДЕЛА ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ С ВНЕДРЕНИЕМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОХРАНЫ И СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Проблема защиты информации существовала всегда, но в настоящее время из-за огромного скачка научно-технического прогресса она прибрела особую актуальность. Поэтому задача специалистов по защите информации, заключается в овладении всего спектра приемов и способов защиты информации, научится моделировать и проектировать системы защиты информации.

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

- непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
- плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
- целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
- конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- активной. Защищать информацию необходимо с достаточной степенью настойчивости;
- надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
- универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
- комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства.

Чем выше уровень безопасности, тем выше вероятность сохранения всех ценностей объекта от хищений или уничтожения. Уровень безопасности, в свою очередь, в основном зависит от того, насколько полно и правильно была разработана инженерно-техническая система защиты информации на предприятии. Другим немаловажным фактором является правильно подобранная система видеонаблюдения, которая усиливает надежность системы безопасности.

Системы телевизионного наблюдения предназначены для обеспечения безопасности на охраняемом объекте. Они позволяют одному или нескольким наблюдателям одновременно следить за одним или многими объектами, находящимися порой на значительном расстоянии как друг от друга, так и от места наблюдения. При этом наблюдения могут производиться в условиях очень низкой освещенности и любой не приемлемой для нахождения людей среды. Компьютерные системы наблюдения предназначены для комплексного управления системой теленаблюдения.

Инженерно-техническая защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности организации или учреждения. Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и

оборудования с помощью комплексов технических средств, иными словами данная система предотвращает утечку какой-либо информации по техническим каналам связи.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей и материальных объектов. Причины утечки связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм, отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Малов С.С., Юмашева Е.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

О КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Во многих организациях используют систему контроля управления доступом (СКУД). Основной задачей СКУД является управление доступом на заданную территорию через некие точки доступа, а также идентификация лица, имеющего доступ на заданную территорию.

Соответственно, в СКУД хранится информация обо всех сотрудниках, которые имеют право прохода на территорию организации, а также посетителях получивших временный пропуск. К этой информации относятся сведения о ФИО, паспортные данные, а иногда и фотография.

Данный набор сведений, согласно Федеральному закону от 27.07.2006г. №152-ФЗ «О персональных данных, относится к персональным данным (ПДн) и, следовательно, должен быть защищен, а СКУД является информационной системой персональных данных (ИСПДн).

При обеспечении защиты ИСПДн необходимо руководствоваться положениями Постановления Правительства РФ от 01.11.2012г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Оно определяет, что перед проектированием системы защиты необходимо используя результаты предпроектного обследования определить уровень защищенности ИСПДн, который определяется по четырем критериям:

1. Тип угроз, актуальных для ИСПДн;
2. Субъект ПДн (сотрудник или не сотрудник организации);
3. Объем обрабатываемых ПДн;
4. Категория обрабатываемых ПДн.

При определении категории ПДн, обрабатываемых в ИСПДн, необходимо руководствоваться нормативно-правовыми актами Российской Федерации. Согласно нормативным документам ПДн могут быть отнесены к одной из следующих категорий:

- специальные;
- биометрические;
- общедоступные;
- иные.

При определении категории ПДн, обрабатываемых в СКУД, сложность возникает с определением необходимости считать ли фотографию биометрическими ПДн, т.к. известно, что к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Это могут быть физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись).

Как уже было отмечено, в СКУД идентификация человека происходит путем сравнения фото на пропуске с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД. Таким образом имеет место быть совокупность использования персональных данных человека.

К сожалению, нормативно-правовая база Российской Федерации не дает однозначного ответа на вопрос, является ли фотография в СКУД биометрическими персональными данными. Что приводило к спорам и субъективным подходам при определении категории ПДн, обрабатываемых в СКУД.

Точку в данном вопросе поставила организация, выступающая в роли регулятора в области защиты персональных данных, - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 30.08.2013г. Роскомнадзор. выпустил "Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки", в которых указал, что «фотографическими изображениями сотрудников организации, содержащимися в системе контроля управления доступа (СКУД), являются биометрическими персональными данными,

поскольку характеризуют физиологические и биологические особенности человека, позволяющие установить, принадлежит ли данному лицу предъявляемый СКУД пропуск, на основе которых можно установить его личность путем сравнения фото с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД».

Таким образом при определении уровня защищенности СКУД, в которой обрабатываются ПДН, нужно учитывать что категория ПДн будет биометрической, а это накладывает дополнительные требования при организации защиты ИСПДн.

Потехин В.С., Ващилова А.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ПУТИ СОЗДАНИЯ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ (ИТ), ОБЕСПЕЧИВАЮЩЕЙ РЕАЛИЗАЦИЮ ПЛАНА «ПЕРЕХВАТ»

Руководство Министерства внутренних дел (МВД) РФ уделяет большое внимание проблемам автоматизации функций управления, возлагаемых на органы внутренних дел (ОВД). Одна из таких функций — поиск автотранспорта в рамках плана «Перехват».

Перехват — общее название для планов, регламентирующих действия органов внутренних дел, по осуществлению неотложных оперативно-розыскных мероприятий при получении сообщения о незаконном завладении автомототранспортным средством, дорожно-транспортном происшествии, с места которого транспортное средство скрылось и пр.

При введении плана «Перехват» создаётся оперативная группа, координирующая все действия в зоне поиска. Для «перехвата» могут привлекаться только силы, штатно участвующие в охране общественного порядка на данной территории («Перехват-1»), а могут быть привлечены дополнительные подразделения («Перехват»). Каждый участник поисковых мероприятий занимает заранее определённую в плане позицию, либо работает по заранее определённому маршруту патрулирования.

Состояние автоматизации процессов, реализующих план «Перехват», можно охарактеризовать следующим.

Получены определенные успехи:

- разработан единый порядок: проведения криминалистических экспертиз; исследований транспортных средств, их узлов и агрегатов, регистрационных и иных документов, а также оплаты сторонним организациям работ, связанных с этим; обеспечивающий информационную поддержку организации работы по розыску транспортных средств в процессе повседневной служебной деятельности сотрудников органов внутренних дел;
- ведется организация и контроль за обучением личного состава методам выявления и задержания транспортных средств, находящихся в розыске;
- определены меры по созданию системы связи, успешно используемой при организации работы по розыску транспортных средств для обеспечения прохождения в установленном порядке оперативной информации о разыскиваемом транспорте.

Но, как показал анализ информации, достигнутый уровень автоматизации плана «Перехват» не в полной мере удовлетворяет современным требованиям, в частности:

- использование крупномасштабных карт, на которых оформляется графическая часть (наносятся условные знаки, обозначения, другие необходимые сведения в зависимости от особенностей обслуживаемой территории) совместно с новыми техническими средствами, принципиально позволяющими ускорить процесс создания графической части плана, малоэффективно;
- в решении нуждаются вопросы оснащения гаражей, стоянок охранной сигнализацией, развитие и внедрение противоугонных средств, а также установки систем видеонаблюдения;
- организация и контроль за своевременностью, полнотой и достоверностью прохождения информации о разыскиваемом транспорте, формирования соответствующих автоматизированных баз данных разрабатывалась без учета новых требований, обусловленных нововведениями в законе.

В этой связи исследования, направленные на создание ИТ, обеспечивающей автоматизацию процессов, реализующих план «Перехват», представляются актуальными и могут осуществляться следующими путями:

- модернизация программного обеспечения фоторадарных комплексов Крис «С» и Арена «С», а также комплексов видеофиксации «Каскад» и «Поток» с целью учета не только данных о нарушениях правил дорожного движения (как это делается сегодня), но и фатографических данных о всех транспортных средствах на рубежах контроля;
- организация сбора фатографических данных (на основе внутриведомственной единой информационно-телекоммуникационной сети МВД РФ) с целью доставки сведений к месту их централизованного хранения;
- организация ведения интегрированной базы упомянутых фактографических данных;

– обеспечение возможности получения по запросу сведений о всех перемещениях конкретного транспортного средства, объявленного в розыск;

– визуализация отобранных данных и их представление в виде, пригодном для проведения оперативно-розыскных мероприятий (например, в табличном виде или путем отображения результатов на карте города).

Реализация названных путей позволит существенно сократить время поиска транспортных средств, объявленных в розыск.

Потехин В.С., Никифорова А.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

ПОДХОД К АВТОМАТИЗАЦИИ КОНТРОЛЯ ДОСТУПА НА ОСОБО ВАЖНЫЕ ОБЪЕКТЫ

Состав особо важных объектов определяется органами государственной власти Российской Федерации или местного самоуправления с целью выработки мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения чрезвычайной ситуации.

Задачи охраны особо важных объектов решаются силами и средствами силовых ведомств, в том числе вневедомственной охраной и внутренними войсками МВД России, преобразуемыми в настоящее время в Федеральную службу войск национальной гвардии Российской Федерации. Одна из задач, стоящих перед МВД России, заключается в контроле доступа на особо важные объекты.

Решение задачи достигается комплексным использованием организационных мероприятий, средств инженерно-технической укрепленности и средствами информационных технологий (ИТ), поддерживающими автоматизацию процессов контроля доступа. Используемые при этом ИТ требуют постоянного совершенствования (из-за создания все новых и новых средств противодействия, а также создания новых элементов ИТ), что и определяет актуальность темы данного исследования.

Конкретный состав средств автоматизации ИТ процессов контроля от объекта к объекту меняется в широких пределах, что определяется спецификой охраняемого объекта, предъявляемыми требованиями и принятыми проектными решениями. При этом на объектах как минимум:

– используют разнообразные датчики (извещатели), которые вырабатывают информацию состояния объектов контроля;

– визуализируют информацию состояния в принятой системе обозначений, которая предоставляется личному составу охраны на пульты контроля или автоматизированные рабочие места (АРМы);

– обеспечивают возможность дистанционной передачи командной информации на исполнительные механизмы контролируемых объектов;

– используют современных средства коммуникаций (в частности, локальную вычислительную сеть), позволяющие интегрировать перечисленные компоненты в единую систему защиты объекта.

Для подержания возможностей ИТ на уровне актуальности представляется целесообразным:

– разработать модель угроз охраняемого объекта и постоянно корректировать эту модель в связи с появлением новых средств, позволяющих преодолевать уже установленные на объекте средства ИТ охраны;

– при выработке проектных решений учитывать:

а) требования, предъявляемые основными руководящими документами, регламентирующими процесс создания средств охраны особо важных объектов, в том числе в части «Защиты от несанкционированного доступа к информации» (ГОСТ Р 50739-95);

б) возможность утраты информации в связи с непреднамеренным или злонамеренным отключением электричества, вследствие чего целостность баз данных, накапливаемых в системе, может быть потеряна;

в) возможность дистанционного считывания служенной конфиденциальной информации (при наличии у злоумышленников специального оборудования);

г) возможность временного воспрепятствования корректной работе датчиков (извещателей) и исполнительных механизмов, работающих по радиоканалам и др.;

д)необходимость автоматического протоколирования всех существенных действий личного состава объекта применяемых аппаратно-программных средств при использовании ИТ с целью последующего анализа и выявления «узких мест» системы охраны объекта;

– своевременно заменять морально устаревшие средства на новые, позволяющие восстановить необходимый уровень защиты;

– создавать резервные схемы защиты, обеспечивающие достаточный уровень дублирования основных элементов защиты объекта (включая источники резервного питания).

Выполнение перечисленных мероприятий позволит поддерживать ИТ на приемлемом уровне и тем самым обеспечивать решение задачи охраны особо важных объектов. Совокупность названных мероприятий можно рассматривать как подход, позволяющий автоматизировать контроль доступа на особо важные объекты с учетом изменяющихся условий эксплуатации.

Потехин В.С., Харрасов Э.Э.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОИСКА УГНАННОГО АВТОТРАНСПОРТА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ РАДИОМЕТОК

Выявление угнанного автотранспорта чаще всего основано на использовании номеров госрегистрации. Но эти номера можно подделать. А отслеживать большое количество номеров в интенсивном автомобильном потоке нелегкая задача. Альтернативу номерам госрегистрации могут составить радиометки – RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) реализующие автоматическую идентификацию объектов, в которых посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Эти метки невозможно подделать без специального дорогостоящего оборудования, да и считывать метки можно сотнями и даже тысячами в секунду на скоростях до 220 км/час. В этой связи тема данной работы представляется актуальной.

Для автоматизации процесса поиска угнанного автотранспорта на основе использования радиометок представляется необходимым:

– на транспортные средства устанавливать радиометки с индивидуальными кодами, автомобиля и наиболее крупных номерных узлов (двигателя, корпуса и др.). Такие метки уже устанавливаются на автомобилях индивидуальной сборки премиум сегмента (хотя эти метки используются производителям лишь в технологических целях). Возможно установка и других радиометок, например, в ключи зажигания. Это тоже может повышать уровень защиты от угона, если считыватель будет находиться в замке зажигания и будет подключен к иммобилайзеру (от англ. immobiliser – «обездвиживатель») – вид электронного противоугонного устройства. Большинство современных автомобилей имеет штатный иммобилайзер, устанавливаемый автопроизводителем. При этом блокирование впрыскивания топлива в двигатель происходит не физически, а программно самой системой контроля двигателя) или бортовому компьютеру;

– организовать централизованный учет (интегрированную базу данных – ИБД) радиметок транспортных средств и их номерных узлов, дополнив этими сведениями традиционные параметры, фиксируемые при регистрации автотранспорта;

– установить стационарные считыватели в точках наиболее интенсивного потока автомобилей, где планируется автоматический контроль движения;

– обеспечить считывание данных радиометок, которые должны быть дополнены текущим временем, координатами установленной антенны считывателя, направлением движения автомобиля и преданы для обработки на ближайший сервер ИБД;

– на сервере:

а) организовать выполнение сравнения поступивших данных с данными автотранспорта, находящегося в угоне. Если результаты проверки положительные, то факт обнаружения зафиксировать в ИБД вместе с сопутствующей информацией. Одновременно на ближайшие посты ГИБДД передается сообщение с информацией достаточной для задержания автомобиля;

б) предусмотреть обработку запросов на выдачу сотрудникам, наделенным необходимыми полномочиями, отчетов по статистике интенсивности движения в районе установки антенн считываля, отчетов о траектории (маршруте) движения конкретного заданного автомобиля. При этом данные выдавать в табличной форме или на фоне карты района поиска;

– проработать вопрос о целесообразности установки приемных антенн на мобильных объектах, например, общественном автотранспорте;

– проработать вопрос о возможности и интеграции данных, получаемых от антенн радиометок, с данными, получаемыми от других технических средств, например, фоторадарных комплексов Крис «С» и Арена «С», комплексов видеофиксации «Каскад» и «Поток».

Представленный перечень действий, конечно, не является исчерпывающе полным, требует дополнительных исследований, но все же позволяет составить общее впечатление о возможном подходе к автоматизации процесса поиска угнанного автотранспорта на основе использования радиометок. Реализация перечисленных мер может способствовать повышению эффективности работы правоохранительных органов с помощью внедрения в систему МВД технических и программных средств автоматизации, реализующих современные информационные технологии.

Примакин А.И., Чудаков О.Е., Рыжков Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

ТЕХНОЛОГИЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО НАЧАЛЬНИКА КАФЕДРЫ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ

В современных условиях поток документов, обрабатываемых подразделениях Университета МВД, увеличивается. Этот поток включает в себя как командную (управляющую) информацию, определяющую организацию образовательного процесса, так и отчетную информацию, которую готовят руководители подразделений в вышестоящие структуры.

В таких условиях справиться с таким потоком информации без использования современных информационных технологий не представляется возможным, что может быть реализовано путем разработки автоматизированных рабочих мест руководителей подразделений. Поскольку основным подразделением высшего учебного заведения является кафедра, прежде всего, целесообразно рассмотреть организацию разработки автоматизированного рабочего места (АРМ) начальника кафедры.

Рабочее место начальника кафедры должно обеспечивать автоматизацию деятельности начальника кафедры по заполнению и ведению всей необходимой документации для периодической отчетности, проведению строгого учета по выполнению задач, поставленных преподавателям, накоплению рейтинговых баллов. Кроме того, данная АРМ содержит полную информацию о каждом из преподавателей, об учебно-методическом комплексе каждой преподаваемой дисциплины.

Для разработки АРМ начальника кафедры необходимо выполнить следующие основные действия:

- провести функциональный анализ деятельности начальника кафедры в течение учебного года с использованием CASE-средств; данный анализ осуществляется на основе изучения деятельности кафедры, потоков информации, циркулирующей между кафедрой и другими подразделениями университета и т.п.;
- разработать структуру базы данных, осуществить нормализацию базы данных, разработать таблицы базы данных, обеспечивающих прием, хранение и формирование всех возможных отчетных документов кафедры;
- разработать структуру интерфейса при решении различных задач кафедры;
- разработать прикладную программу для обеспечения работы с базой данных, формирования отчетных документов и др. функциональные задачи начальника кафедры.

Создание данного АРМ позволит эффективно обрабатывать большие потоки информации, которые имеют определенную структуру, зависящую от места применения

Для решения поставленной цели были решены следующие задачи: изучена деятельность начальника кафедры; проанализированы информационные потоки, относящиеся к деятельности преподавателей и кафедры в целом; изучены специальные задачи и обязанности личного состава кафедры специальных информационных технологий; проведено обоснование проектного решения по созданию АРМ начальника кафедры; спроектировано АРМ начальника кафедры; проведена пробная эксплуатация, созданного АРМ.

Благодаря АРМ значительно повышается скорость поиска, обработки информации, а так же повышается скорость принятия решений начальника кафедры, а сами решения становятся более обоснованными. Интерфейс системы настолько прост и интуитивно понятен, что даже те руководители, которые ранее минимально использовали информационные технологии в своей работе, смогут быстро освоить АРМ и применять его на практике. Система АРМ, являющаяся человеком-машиной, должна быть открытой, гибкой, приспособленной к постоянному развитию и совершенствованию. В такой системе должны быть обеспечены: максимальная приближенность специалистов к машинным средствам обработки информации; работа в диалоговом режиме; хорошая производительность компьютера; максимальная автоматизация рутинных процессов; возможность самообучения специалистов.

Задачи, решаемые АРМ можно разделить на информационные и вычислительные.

К информационным задачам относятся кодирование, классификация, сбор, структурная организация, корректировка, хранение, поиск и выдача информации. Часто информационные задачи включают несложные вычислительные и логические процедуры арифметического и текстового характера и отношения (связи). Информационные связи, как правило, являются наиболее трудоемкими и занимают большую часть рабочего времени.

Вычислительные задачи являются как формализуемыми, так и не полностью формализуемыми. Формализуемые задачи решаются на базе формальных алгоритмов и делятся на две группы: задачи прямого счета и задачи на основе математических моделей. Задачи прямого счета решаются с помощью простейших алгоритмов. Для более сложных задач требуется применять различные математические модели. В последнее время большое внимание выделяется разработке средств решения не полностью формализуемых задач, называемых систематическими. Такие задачи возникают очень часто в ходе управления, особенно при принятии решения в условиях неполной информации.

Данное АРМ будет обеспечивать высокую надежность технических средств, организацию удобных для пользователей режимов работы, способность обрабатывать в заданное время необходимый объем данных. Поскольку АРМ является индивидуальным пользовательским средством, оно должно обеспечивать высокие эргономические свойства и комфортность обслуживания. Применение данной технологии позволит получить АРМ начальника кафедры, которое обеспечит возможность хранения и обработки всей необходимой информации в рамках одного программного пакета, повышение оперативности работы начальника кафедры, а также повысит эффективность принимаемых им решений.

Родин В.Н., Томашевич Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

ОБОСНОВАНИЕ И ВЫБОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОБЪЕКТОВ ОВД

В работе предложена методика обоснования и выбора требований к информационным технологиям для обеспечения защиты объектов в органах внутренних дел.

Рассмотрим важные в этой системе определения для обеспечения защиты объектов органов внутренних дел:

– Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (ФЗ № 149-ФЗ; приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных (ГОСТ 34.003-90); ресурсы, необходимые для сбора, обработки, хранения и распространения информации.

– Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Система защиты информации. Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Существуют различные виды защиты информации:

1. Физическая защита информации. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

2. Правовая защита информации. Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

3. Техническая защита информации. ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

4. Криптографическая защита информации. Защита информации с помощью ее криптографического преобразования.

Способ защиты информации:

1. Защита информации от утечки. Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней.

2. Защита информации от несанкционированного воздействия. ЗИ от НСВ: Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3. Защита информации от непреднамеренного воздействия. Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

4. Защита информации от разглашения. Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

5. Защита информации от несанкционированного доступа.

6. Защита информации от преднамеренного воздействия. Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

7. Защита информации от [иностранной] разведки. Защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Таким образом, тема этой работы является актуальной, ее можно рассматривать в различных сферах информационных технологий.

Савченко-Новопавловская С.Л., Дикий Д.И.
Россия, Санкт-Петербург, Университет ИТМО

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Проблема защиты информации в сети Интернет крайне актуальна, однако на данный момент недостаточно разработана. В частности, в рамках современного национального и международного права отсутствует эффективный механизм правовой защиты интеллектуальной собственности в киберпространстве.

Развитие института правовой защиты интеллектуальной собственности сопряжено с рядом проблем, обусловленных спецификой сущности сети Интернет. Поскольку интернет-сфера является технической системой, любые технические стандарты в определенной степени ограничивают киберпространство. Следует обратить внимание, что инновационные решения в технологической сфере не всегда влекут серьезные правовые последствия, поэтому современные ученые и практикующие юристы сходятся во мнении, что в настоящее время целесообразно определить международный контроль за введением и соблюдением технических стандартов со стороны государств.

Проблемой является отсутствие четкого определения сущности веб-сайта, как объекта интеллектуальной собственности. Закон об информации дает следующие определение сайта в сети Интернет: «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»». При этом данное определение не отражает сущности веб-сайта с позиции права интеллектуальной собственности. Ни в теории, ни в законодательстве не разработана характеристика сайта, как комплексного объекта интеллектуальной собственности. Законодатель определяет лишь отдельные объекты, расположенные на веб-сайте (изображения, тексты, аудиовизуальные материалы, программное обеспечение и т.д.).

Предлагаются следующие способы решения проблем правовой защиты интеллектуальной собственности в Интернет-пространстве. В первую очередь, необходимо активное международное сотрудничество, целью которого является унификации нормативных правил. Иными словами, следует провести интеграцию правовых систем для единообразной регламентации Интернета, как международной компьютерной сети и установлении целостного механизма юридической ответственности за нарушения, объектом которых являются результаты интеллектуальной деятельности.

Некоторые методы решения проблем обеспечения защищенности результатов интеллектуальной деятельности в сети Интернет необходимо реализовать на уровне конкретных пользователей, к примеру, владельцев коммерческих веб-сайтов.

На стадии разработки веб-сайта в целом или отдельных его элементов (текста, изображений и т.д.) следует позаботиться о документальном закреплении факта отчуждения исключительного права на весь контент, расположенный на нем, в пользу владельца сайта. Также, важно предусмотреть в трудовых и гражданско-правовых договорах обязанность всех временных или постоянных работников использовать средства технической защиты при работе с веб-сайтом компании.

Наконец, важно использовать обозначения, служащие для индивидуализации товаров юридических лиц или индивидуальных предпринимателей, которые следует зарегистрировать официально. В перспективе на предприятии следует разработать политику безопасности, которая будет включать в себя правила работы с веб-сайтом компании.

Синещук Ю.И., Конопак А.Е.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России

ОРГАНИЗАЦИЯ ЗАЩИЩЕННЫХ КАНАЛОВ СВЯЗИ НА БАЗЕ ТЕХНОЛОГИИ VIPNET В МЧС РОССИИ

Автоматизированная информационная управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее - АИУС РСЧС), объединяя ресурсы различных информационных систем, позволяет МЧС России эффективно реализовывать свои функции как координатора, обеспечивающего взаимодействие органов государственного управления при решении задач в условиях чрезвычайных ситуаций. АИУС РСЧС строится на принципах функционирования открытых систем и выступает в качестве ядра системы с собственной базой агрегированных данных и территориально-распределенных источников детальной и оперативной информации.

В соответствии с российским законодательством автоматизированные системы, обрабатывающие сведения ограниченного доступа, должны выполняться в защищенном исполнении. Поэтому проблема обеспечения конфиденциальности, целостности и доступности информационных,

вычислительных и коммуникационных ресурсов АИУС РСЧС является актуальной и предполагает решение задачи безопасного взаимодействия различных подсистем РСЧС в рамках подключения к ведомственной цифровой сети связи(ВЦСС) МЧС России.

В общем случае, при всех таких подключениях могут применяться либо штатные средства разграничения доступа операционной системы, либо специализированные средства защиты от НСД, либо криптографические системы на уровне конкретных приложений, либо и то и другое вместе. Однако все эти меры, в силу присущих им ограничений, не могут гарантировать желаемой безопасности при проведении сетевых атак. Как следствие, необходимо обеспечить на сетевом уровне тотальный контроль всего входящего и исходящего трафика компьютера, проходящего через все его сетевые интерфейсы с реализацией функций шифрования и имитозащиты трафика, а также функций персонального межсетевого экрана.

При построении защищенных сетей МЧС России широкое применение находит программно-аппаратный комплекс ViPNet (ViPNet Administrator, ViPNet Client, ViPNet Coordinator), позволяющий сформировать среду безопасного обмена информацией по общедоступным каналам связи различных типов путем создания логических сетей, защищенных криптографическими средствами высокой надежности.

Развертывание частных виртуальных сетей(Virtual Private Network – VPN) любых конфигураций, обеспечивающих прозрачное взаимодействие компьютеров сети ViPNet независимо от способа, места и типа IP-адреса при их подключении к сети, позволяет добиться защиты всего сетевого трафика. Сеть ViPNet, в которой используется технология VPN, обладает следующими возможностями: плавная интеграция в структуру существующей сети; гибкая настройка фильтрации защищенного и открытого трафика; централизованное управление политиками безопасности; широкий выбор средств коммуникации между защищенными узлами (почта, чат, обмен файлами); организация юридически значимого электронного документооборота; система слежения за состоянием сети; организация иерархической системы сетей; дополнительные возможности по регистрации пользователей, публикации сертификатов в общедоступных хранилищах и другие.

Построение сетей ViPNet на базе частных виртуальных сетей – процесс, имеющий свои особенности в каждом конкретном случае. В первую очередь он зависит от существующей топологии сети и от тех коммуникационных задач, которые стоят перед организацией. Именно поэтому универсальной схемы сети ViPNet не существует.

В каждом региональном центре МЧС России развернута своя сеть ViPNet с уникальным номером. Эти сети образуют иерархическую структуру подчинения, что накладывает определенные проблемы на их взаимодействие между собой. Установление соединения между двумя узлами сети ViPNet требует, чтобы эти узлы обладали информацией о параметрах доступа друг к другу. Для решения этой задачи можно связать каждый координатор со всеми координатами своей и чужих сетей. Но в больших сетях, каковой является сеть МЧС России, это приведет к загрузке каналов служебной информацией, а координаторы будут загружены ее обработкой. В связи с этим определение необходимых связей между различными узлами всех сетей ViPNet МЧС России и установление соединений между этими узлами предполагает модернизацию сети ViPNet МЧС России в следующих направлениях:

- установление межсетевого взаимодействия всех сетей ViPNet МЧС России;
- дооснащение подразделений МЧС России программно-аппаратными комплексами ViPNet Coordinator для создания защищенных каналов связи со всеми субъектами МЧС России.

Решение сформулированных задач позволяет: сетевым узлам, находящимся в разных сетях ViPNet, установить между собой соединения так, как если бы они находились в одной сети ViPNet; значительно сократить расходы на аренду каналов у операторов связи; повысить защищенность передаваемой по каналам связи информации.

Синещук Ю.И., Левчунец И.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России

ОБОСНОВАНИЕ СИСТЕМЫ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В МНОГОУРОВНЕВОЙ НАВИГАЦИОННО-ИНФОРМАЦИОННОЙ СИСТЕМЕ МОНИТОРИНГА ТРАНСПОРТНЫХ СРЕДСТВ МЧС РОССИИ НА БАЗЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ГЛОНАСС

Развитие и повсеместное применение информационных технологий, использование глобальных навигационных спутниковых систем является закономерной тенденцией мирового развития. Вместе с тем, применение новых информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести значительный ущерб пользователям. Применительно к автоматизированным системам МЧС России, речь может идти не только о материальном, экономическом и культурном ущербе, но и об экологическом, социальном и или политическом ущербе.

В последние годы, в связи началом полномасштабного использования навигационных спутниковых систем для нужд государства, промышленности и потребительского сектора экономики, особую актуальность приобретают вопросы стандартизации процедур обеспечения информационной безопасности. В интересах государственных органов Российской Федерации предпочтение в вопросах навигационных систем отдается отечественной системе ГЛОНАСС. Система ГЛОНАСС, являясь навигационной системой двойного назначения, обеспечивает решение навигационных и координатно-временных задач в интересах как специальных, так и гражданских потребителей. В рамках развития многоуровневой навигационно-информационной системы (МНИС) мониторинга транспортных средств МЧС России, оборудованных аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS, задача обеспечения конфиденциальности, целостности и доступности информационных, вычислительных и коммуникационных ресурсов системы является актуальной. МНИС предназначена для обеспечения автоматизации процессов мониторинга транспортных средств, предупреждения и ликвидации чрезвычайных ситуаций, тушения пожаров, ликвидации последствий происшествий на водных объектах, а также процессов сбора, визуализации, анализа навигационной и служебной информации в целях принятия управленческих решений.

В общем случае, порядок выбора мер защиты информации для их реализации в информационной системе включает:

– определение базового набора мер защиты информации для установленного класса защищенности информационной системы;

– адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы;

– уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

– дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

В соответствии с руководящими документами уточненный адаптированный базовый набора должен включать следующие меры защиты информации:

– идентификация и аутентификация субъектов доступа и объектов доступа;
– управление доступом субъектов доступа к объектам доступа;
– ограничение программной среды;
– защита машинных носителей информации;
– регистрация событий безопасности;
– антивирусная защита;
– обнаружение (предотвращение) вторжений;
– контроль (анализ) защищенности информации;
– обеспечение целостности информационной системы и информации;
– обеспечение доступности информации; защита среды виртуализации;
– защита технических средств;
– защита информационной системы, систем связи и передачи данных.

Комплексное применение предложенных мер защиты позволит обеспечить требуемый уровень информационной безопасности МНИС и повысить эффективность ее применения.

Соловейчик М.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ-ПОИСКОВЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ДЕЯТЕЛЬНОСТИ ЦЕНТРОВ ВРЕМЕННОГО СОДЕРЖАНИЯ НЕСОВЕРШЕННОЛЕТНИХ ПРАВОНАРУШИТЕЛЕЙ

Одной из тревожных проблем в России является ситуация с безнадзорными несовершеннолетними, совершающими противоправные деяния.

Центр временного содержания для несовершеннолетних правонарушителей (далее – ЦВСНП), осуществляет профилактическую работу с несовершеннолетними, доставленными за совершение правонарушений и нуждающихся в специальном вмешательстве государства для профилактики противоправного поведения последних. В процессе исполнения служебных обязанностей сотрудники ЦВСНП могут использовать информационно-поисковые системы ОВД. Как правило, в этом возникает необходимость при затруднении в установлении личности или иных характеризующих данных о доставленных несовершеннолетних.

В случае доставления в ЦВСНП несовершеннолетних, личность которых не установлена, должностные лица ЦВСНП принимают меры к их установлению. В этих целях должностные лица

ЦВСНП выявляют обстоятельства задержания несовершеннолетних доставленных, путь их следования, вид транспорта, места возможного проживания, источники и средства существования, а также иные обстоятельства, имеющие значение для установления их личности.

Для установления личности составляется описание внешности по методу словесного портрета, организуют фотографирование несовершеннолетних (фас, оба профиля), а также составляют описание одежды и других имеющихся у них вещей.

Собранная информация проверяется через информационно-поисковые системы органов внутренних дел, в которых собрана информация о лицах, объявленных в розыск и о лицах, пропавших без вести.

Согласно ФЗ №3 «О полиции» внесению в банки данных полиции подлежит так же информация о несовершеннолетних:

- освобожденных от уголовной ответственности либо освобожденных судом от наказания с применением принудительных мер воспитательного воздействия;
- о несовершеннолетних, совершивших правонарушения и (или) антиобщественные действия,
- о родителях или иных законных представителях, не исполняющих своих обязанностей по воспитанию, обучению и (или) содержанию детей и (или) отрицательно влияющих на их поведение либо жестоко обращающихся с ними.

На несовершеннолетних, помещенных в ЦВСНП, заводятся учетно-статистические дела. Также указанная информация вносится в автоматизированные информационно-поисковые системы МВД России.

Таким образом, информационно-поисковые системы играют значительную роль в деятельности ЦВСНП, помогая установить личность доставленного несовершеннолетнего. Однако и сотрудники ЦВСНП способны пополнить банки данных, что может произойти при активной и результативной работе с несовершеннолетними, заключающейся в проведении опроса со знанием психологических особенностей доставленных подростков. Пополнение информации способствует более эффективной деятельности по профилактике безнадзорности и правонарушений несовершеннолетних в Российской Федерации.

Помимо помощи в профилактике подростковой преступности по стране в целом, следует обратить внимание, что ЦВСНП субъектов России являются носителями информации о подростках со времен Великой отечественной войны. Она часто бывает необходима уже взрослым людям, например, для подтверждения определённого социального статуса. Однако, данные сведения не занесены в централизованные информационные ресурсы МВД и их сохранность зависит от отношения к служебным обязанностям сотрудников конкретного ЦВСНП.

Хомченкова А.О., Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗАЦИИ КОНТРОЛЯ ПРОЦЕССА УПРАВЛЕНИЯ ПРИБЫТИЯ ЛИЧНОГО СОСТАВА ПО ТРЕВОГЕ В УНИВЕРСИТЕТ МВД РФ

Одним из основных требований, предъявляемых к сотрудникам Министерства Внутренних Дел Российской Федерации, является высокая боеготовность, в связи с чем, в университете периодически объявляются различные тревоги, обеспечивающие поддержание боеготовности сотрудников МВД.

Основой процесса управления прибытия личного состава по получению сигнала в университет является решение начальника (командира). Как правило, начальник территориального органа (университета) подает сигнал о тревоге, в соответствии с которым личный состав должен прибыть в территориальный орган (университет). В большинстве территориальных органов МВД РФ существуют специальные аппараты, с помощью которых происходит оповещение. В Санкт-Петербургском университете МВД РФ на данный момент такого аппарата нет, поэтому оповещение происходит более длительно, чем могло бы. На основе этого, предлагается создать автоматизированную информационную систему, с помощью которой оповещение личного состава будет происходить более структурировано, быстро и безопасно. Необходимо создать схему оповещения личного состава, в которой нужно указать должность, звание, фамилию, имя, отчество, номер телефона и адрес фактического проживания каждого сотрудника. Как правило, оповещение происходит от высшего начальства к низшему. Начальники оповещают своих заместителей, заместители – подчиненных и т. д.

В условиях многогранной деятельности командира необходимо учитывать различные условия деятельности подразделения. Для каждого сотрудника установлено различное время прибытия по сигналу тревоги в соответствии с местом его фактического проживания.

В каждом подразделении установлен определенный набор вещей, с которыми сотрудник должен прибыть по сигналу (такие как паспорт, продукты питания, одежда и т. д.). Сотрудники всегда должны быть готовы по сигналу тревоги прибыть не только в подразделение для проверки

боеготовности, но и выдвинуться на какие-либо учения на неопределенный срок, если это необходимо.

Для повышения показателя эффективности реализации решения командира при управлении подразделением используют различные средства автоматизации. В настоящее время информационные системы и технологии очень активно развиваются, распространяются и присутствуют в жизни каждого человека. В связи с этим, внедрение новых информационных систем и технологий в жизнь сотрудников ОВД принесет большую пользу и облегчит некоторые аспекты деятельности сотрудников различных подразделений.

Самостоятельный научный практический интерес представления автоматизации процесса управления личным составом по тревоге связан с необходимостью обеспечить своевременное и качественное информирование личного состава по необходимости.

Предполагается схема управления сбора по тревоге, но, несмотря на это, существует угроза срыва процесса передачи данных. Для исключения таких ситуаций необходимо разработать модель, которая обеспечивает безопасность информации в автоматизированной системе управления контроля учета прибытия личного состава по тревоге.

В работе предложена модель, которая распознает угрозы и способствует устранению этих угроз. Для создания указанной модели, необходимо провести объемную информационно-аналитическую работу. Информационно-аналитическая работа - непрерывное добывание, сбор, изучение, отображение и анализ данных об обстановке. Для проведения корректной информационно-аналитической работы, требуется формирование адекватной модели управленческого решения, основанной на установлении формальной аналитической зависимости между тремя базовыми компонентами управленческого решения.

Чудаков О.Е., Хахель С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

РАЗРАБОТКА ЭЛЕМЕНТОВ СИСТЕМЫ, АВТОМАТИЗИРУЮЩИХ ПРОЦЕСС ВЫЯВЛЕНИЯ И УЧЕТА ПРАВОНАРУШЕНИЙ НА ВОДНЫХ МАГИСТРАЛЯХ ГОРОДА С ИСПОЛЬЗОВАНИЕМ КВАДРОКОПТЕРОВ

Издавна и по сей день распространенность водного транспорта довольно высока и продолжает расти. Грузоперевозки, туризм, а так же частный водный транспорт в городах можно видеть повсюду. Но при распространении этого типа транспорта, в том числе с использованием маломерных судов, увеличивается и количество правонарушений с их участием, а выявление этих правонарушений довольно затруднительно т.к. безопасность на водных магистралях развита недостаточно, да и выделение большого количества ресурсов не всегда позволяет эффективно решить поставленную задачу.

Контроль и управление обеспечением безопасности движения водного транспорта осуществляется определенными службами на основании информации о состоянии водной среды. На основе анализа поступающей информации человеком (лицом принимающим решения) принимаются решения о принимаемых мерах (по управлению безопасностью). Качество принимаемых решений в данном случае существенно зависит от наличия и качества информации, характеризующей обстановку. Одним из важнейших свойств этой информации являются достоверность и оперативность. Кроме того, необходимо иметь соответствующие программные средства обработки данной информации.

Одним из перспективных направлений формирования данной информации может быть использование квадрокоптера с устройством видео фиксации, а также поддержкой передачи видео и других данных по web каналу (интернет). Также потребуется база данных для учета и хранения полученной информации.

Использование квадрокоптера в процессе выявления и учета правонарушений на водных магистралях города позволяет получить следующее:

1) Оперативную и достоверную информацию.
2) Мобильность.

Для учета и хранения правонарушений, а также ведение статистики потребуется разработать базу данных.

Совокупность рассмотренных фактов потребует решения следующей задачи:

1) Разработать модели и алгоритмы для реализации процесса выявления правонарушений на водных магистралях города.
2) Передача по web каналу полученной информации.
3) Построение БД для учета правонарушений на водных магистралях.

Таким образом, предлагаемый вариант совершенствования системы получения информации о водной среде и направлений совершенствования программного обеспечения ее обработки позволят повысить оперативность и достоверность принимаемых решений по управлению безопасностью на водных магистралях города.

Целовальников Н.А., Пушкина О.А., Пенкин Д.Д.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

КОМПЛЕКСНАЯ ОЦЕНКА ДЕЯТЕЛЬНОСТИ КУРСАНТОВ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА (НА ПРИМЕРЕ КЛАСТЕРНОГО АНАЛИЗА)

Современный специалист должен хорошо ориентироваться в вопросах количественного описания вероятностных процессов, находить закономерности в случайных явлениях, владеть навыками обработки и интерпретации статистических данных, уметь применять количественные методы анализа и прогнозирования развитий различных процессов или явлений в своей предметной области.

В тезисе авторы демонстрируют возможность получения комплексной оценки деятельности курсантов факультета подготовки сотрудников для оперативных подразделений (в частности, по специальностям «Безопасность информационных технологий в правоохранительной сфере» и «Информационные системы и технологии») Санкт-Петербургского университета МВД России, взяв за основу методы многомерного анализа (на примере кластерного анализа).

Кластерный анализ предназначен для разделения неоднородной совокупности, элементы которого характеризуются многими признаками, на однородные или близкие по определенным критериям группы.

Основными этапами кластерного анализа являются:

1. Отбор выборки объектов для кластеризации.
2. Выделение признаков, характеризующих каждый объект данной совокупности, получение их числовых значений. При необходимости – нормализация значений признаков.
3. Определение меры близости между объектами и группами объектов.
4. Создание групп сходных объектов (кластеров).
5. Представление результатов кластеризации.
6. Анализ результатов кластеризации и при необходимости корректировка выбранной метрики (п. 3) и метода кластеризации (п. 4) до получения оптимального результата.

На первом этапе применяют выборочный метод математической статистики, с помощью которого формируется выборка объектов для дальнейшего исследования. Для комплексной оценки курсантов в качестве объектов мы используем взвода факультета.

На втором этапе происходит выбор признаков, по которым будет проводиться кластеризация. В качестве признаков мы используем средние показатели курсантов по успеваемости и физическому развитию.

На третьем этапе определяется метрика или мера близости между объектами и мера близости между группами объектов. Расстояние между кластерами может определяться по нескольким правилам, например: принцип «ближайшего соседа», принцип «дальнего соседа», принцип «средней связи».

На четвертом этапе из объектов образуем кластеры: по оси x отмечается средний показатель по успеваемости взвода, по оси y отображается средний показатель по физической подготовки взвода.

На пятом этапе, на основании кластеров, мы определяем 3 группы подготовленности взводов по успеваемости и физической подготовке:

- взвода с высоким показателем;
- взвода со средним показателем;
- взвода с низким показателем.

По результатам кластеризации мы можем сделать вывод: третьей группе взводов с низким показателем необходимы дополнительные занятия по физической подготовке, а так же необходимо усилить контроль проведения самоподготовки к занятиям, второй группе взводов необходимы факультативные занятия по отстающему показателю (физическая подготовка, успеваемость по учебным дисциплинам) для поддержания и улучшения текущих показателей успеваемости, первая группа взводов должна продолжать показывать высокие показатели в учебе и физической подготовке и служить примером для остальных взводов.

Метод кластерного анализа позволяет разделить неоднородную совокупность наблюдаемых объектов на однородные группы и классифицировать эти группы.

Таким образом, мы смогли разделить взвода одного факультета на 3 группы, из которых можно сделать выводы об общей успеваемости факультета и составить план по улучшению показателей отдельных взводов.

Якушев Д.И., Жидкова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

АВТОМАТИЗАЦИЯ ПРОЦЕССА СБОРА ДАННЫХ РЕЗУЛЬТАТОВ ПРОТОКОЛИРОВАНИЯ СОБЫТИЙ БЛИЗ ДВИЖУЩЕГОСЯ ОБЩЕСТВЕННОГО ТРАНСПОРТА

С развитием интернет технологий (Web-технологий) происходит автоматизация многих направлений жизнедеятельности человека, что влечет за собой повышение контроля, например, в соблюдении правил дорожного движения. На основе внедрения Web-технологий в сфере безопасности дорожного движения (БДД) происходит мониторинг соблюдения правил дорожного движения (ПДД).

БДД – состояние защищенности участников дорожного движения от дорожно-транспортных происшествий и их последствий. Обеспечение безопасности дорожного движения – деятельность, направленная на предупреждение причин возникновения дорожно-транспортных происшествий, снижение тяжести их последствий.

Web-технологии позволяют совершенствовать процесс управления БДД. Для этого необходимо разработать модель управления БДД, учитывающую возможности Web-технологий.

В статье рассматривается автоматизированная система сбора данных результатов протоколирования событий близ движущегося общественного транспорта. Для сбора данных необходимы такие средства как: спутниковая система навигации – ГЛОНАСС; видеорегистраторы обстановки в салоне и перед транспортным средством; системы видеоконтроля скорости, а также сети передачи данных.

Вся информация поступает в единый диспетчерский центр (ЕДЦ) управления пассажирским сегментом транспортного комплекса, который предназначен для аналитической и информационной поддержки решения задач управления транспортом.

Основными целями ЕДЦ являются:

1. Повышение эффективности процессов управления функционированием пассажирского транспорта, информационной среды и комплекса информационных услуг.
2. Повышение уровня безопасности в сегменте пассажирского транспорта на базе получения полной, достоверной и оперативной информации о происходящих изменениях и событиях, своевременного выявления негативных тенденций.

Для достижения указанных целей ЕДЦ должен решать следующие задачи:

1. Мониторинг пассажирского сегмента транспортного комплекса.
2. Контроль безопасности работы пассажирского транспорта.
3. Управление транспортным комплексом в чрезвычайных ситуациях.
4. Управление пассажирским транспортом на основе технологий электронного обмена данными.

Данные, поступающие за сутки, достигают больших объемов, что требует максимального упорядочения хранения на серверах ЕДЦ. Для этого необходимы аппаратные, программные и организационные средства:

1. Формирование базы данных определенного маршрута, в котором имеются данные о каждом транспортном средстве (индивидуальный государственный регистрационный знак), курсирующего на этом маршруте.
2. Web-сервер.
3. Сервер сбора и обработки информации.
4. Сервер создания и хранения архивов (данные различных видов должны храниться раздельно, например, видеоматериалы из салона хранятся отдельно от видеоматериалов дорожной обстановки и т. п.).
5. Сети передачи данных.

С развитием Web-технологий осуществляется автоматизация процессов управления БДД. На основе моделей управления БДД с применением Web-технологий происходит мониторинг условий адекватной деятельности участников дорожного движения. Средством реализации мониторинга является – автоматизированная система, которая позволяет принимать управленческие решения, соответствующие сложившейся дорожной обстановке.

Якушев Д.И., Иванова Е.А., Мордовина А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,

ПРИМЕНЕНИЕ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА (НА ПРИМЕРЕ КЛАСТЕРНОГО АНАЛИЗА) В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОВД

В настоящее время требуется новый подход к вопросам обеспечения информационной безопасности в ОВД, учитывающий современный уровень систем защиты информации (СЗИ). Основная причина возникновения проблем в области информационной безопасности – это низкий уровень подготовки сотрудников в области защиты информации. Часто применяются весьма дорогостоящие технические средства и внедряются строго регламентированные организационные

мероприятия. Однако нет ответа на важный вопрос - насколько предлагаемое или уже реализованное решение хорошо, какова его планируемая или реальная эффективность. Такому положению препятствует ряд причин:

- игнорирование системного подхода как методологии анализа и синтеза СЗИ;
- отсутствие механизмов полного и достоверного подтверждения качества СЗИ;
- недостатки нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев.

Устранению этих причин частично может способствовать применение к анализу угроз информационной безопасности современного математического аппарата кластерного анализа, который позволяет выявить наиболее вероятные угрозы информационной безопасности, как на текущий момент, так и в перспективе.

Метод кластерного анализа состоит в исследовании множества количественных факторов, влияющих на информационную безопасность объекта. На первом этапе исследования проводится проверка однородности множества влияющих факторов, а в случае ее отсутствия – разделение этого множества на однородные группы, пригодные для дальнейшего исследования. При этом группы подбираются таким образом, чтобы внутри каждой из них оказывались «похожие» объекты, а объекты разных групп существенно отличались друг от друга.

Кластеры подбираются по следующим правилам:

- каждый элемент первоначальной совокупности принадлежит только одному кластеру;
- элементы, принадлежащие одному и тому же кластеру сходны по рассматриваемым признакам;
- элементы разных кластеров различаются по рассматриваемым признакам.

Совокупность рассматриваемых признаков определяется сотрудником, ответственным за информационную безопасность, исходя из постановки решаемой проблемы.

Например, при решении задачи анализа совокупности зарегистрированных преступлений специалисты по обеспечению информационной безопасности могут прийти к выводу о необходимости разделения всех исследуемых объектов на группы с приблизительно равными определяющими показателями и признаками, а затем внутри каждой группы провести исследование влияния и взаимосвязи различных признаков, определяющих уровень безопасности.

В процессе кластеризации возникает задача нахождения расстояния не только между объектами, но и между группами (кластерами) объектов, для четкого обозначения границ между группами объектов по их индивидуальным характеристикам. Расстояние между кластерами может определяться, например, по следующим принципам: «ближайшего соседа», «дальнего соседа», «средней связи».

Сфера использования кластерного анализа очень широка. Всякий раз, когда необходимо систематизировать значительный объем информации и привести его к пригодным для дальнейшей обработки группам, кластерный анализ оказывается весьма полезным и эффективным. Его применение позволяет конкретизировать предпосылки совершения преступлений в сфере информационных технологий, что предоставляет возможность для разработки индивидуальных подходов и методов не только для раскрытия совершенных преступлений, но и для пресечения некоторых из них на стадии подготовки.

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Алексеев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЩИЙ ИНФОРМАЦИОННЫЙ РЕСУРС, ФУНКЦИИ И ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ПОДРАЗДЕЛЕНИЯМИ ОВД

Работы по созданию общего информационного ресурса (ОИР) ОВД следует начинать с комплексного обследования существующей системы управления в ОВД субъекта федерации, при котором основное внимание должно быть уделено упорядочению информационных ресурсов, документооборота и обмена информацией между органами управления всех уровней. Следует унифицировать описания информационных ресурсов (ИР), что позволит создать условия для их интеграции в ОИР, удобства их поиска и использования должностными лицами, повышения качества информационного взаимодействия с вышестоящими АСУ и нижестоящими компьютерными сетями подразделений управления.

Работы по упорядочению ИР ОВД должны включать выявление связей и анализ информационного взаимодействия между органами управления, уточнение процессов управления, в выполнении которых они участвуют, и определение ИР, необходимых для реализации процессов управления.

Важнейшим направлением создания ОИР территориальных ОВД является разработка унифицированного информационно-лингвистического обеспечения (ИЛО) интегрированных АСУ в ОВД субъекта федерации.

В свою очередь, ИР всех уровней управления в совокупности образуют ОИР ОВД субъекта федерации. ОИР ОВД должно обеспечивать управление в рамках компьютерных сетей (КС) подразделений ОВД с общими функциями управления, с едиными правилами создания и использования информации, с едиными стандартами представления документов и возможностью непосредственного доступа к ним операторского состава АРМ в соответствии с имеющимися полномочиями.

Согласование и унификация ИР должны осуществляться как по адресации, так и по наименованию. При этом по адресации должны осуществляться согласования:

1) перечней адресов объектов распространения и потребления ИР;
2) форматов адресов объектов (алфавит, система счисления, код, длина в знаках);
3) правил адресации.

По наименованию должны осуществляться согласования:

1) по правилам наименования ИР (грамматика, синтаксис),
2) форматам имен ИР (алфавит, система счисления, код, длина в знаках).

Разработка адресации и наименования должна вестись с использованием таблиц соответствия адресов и имен, программ преобразования адресов и имен ИР из одного формата в другой.

Функции управления сложной социальной организационно-технической системы (СОТС) в виде подразделений ОВД реализуются в ходе информационных процессов, организуемых органами управления посредством информационных технологий (совокупности методов, способов, процессов, приемов обработки ИР). При этом сам информационный процесс реализации функции управления должен быть задан или электронным регламентом, или системным алгоритмом. Следовательно, совокупность функций управления и информационных технологий их реализации могут представлять собой первый элемент интегрированной информационной среды управления (ИИСУ) подразделениями ОВД как СОТС.

Еще одним направлением создания ОИР является развитие (создание) телекоммуникационных систем, позволяющих обеспечивать органам управления (должностным лицам) доступ к соответствующим территориально-разделенным ИР в подразделениях ОВД. Необходимо проведение стандартизации, унификации и сертификации программно-технических средств и телекоммуникационных систем, обеспечивающих ОИР.

Для решения всего комплекса задач по созданию ОИР в ОВД субъекта федерации необходимо:

1. Обеспечить тесную кооперацию усилий органов управления ОВД, научно-исследовательских организаций и промышленных предприятий.

2. Кардинально пересмотреть методы, средства формирования, поиска, передачи, использования и защиты информации, применяемые при отсутствии как ИАСУ ОВД, так и ОИР.

3. Убедить руководство ОВД в том, что создание и внедрение ОИР в рамках КС позволит обеспечить качественно новый уровень реализации информационных технологий на всех уровнях управления.

Полнота и достаточность ИР должна обеспечиваться, исходя из необходимости выполнения заданных функций управления, а также управления заданными классами объектов. Формы существования ИР должны соответствовать видам базовых (унифицированных) компьютерных технологий: файлы фактографических БД, документы (текстовые, графические, мультимедийные), файлы БД сетевых графиков, гипертекст.

Баранов Н.А.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ИНФОРМАЦИОННАЯ ПОЛИТИКА РОССИИ В КОНТЕКСТЕ КОНЦЕПЦИИ «МЯГКОЙ СИЛЫ»

После окончания «холодной войны» возросла популярность «мягкой силы», свидетельствующей о привлекательности западной модели развития. Однако события конца XX – начала XXI вв. свидетельствуют о сдвиге парадигмы влияния на современные политические процессы. Действенность мягкой силы стала ставиться под сомнение, и акцент теперь сосредоточен на сочетании «твердой силы» для принуждения и возмездия с «мягкой силой» в виде убеждения и притяжения. Джозеф Най, не отказываясь от использования «мягкой силы», пишет в своей работе «Будущее власти» о необходимости сочетания ресурсов для реализации поставленных целей с использованием полного набора инструментов: дипломатических, экономических, военных, политических, правовых, культурных, коммуникационных, применение которых может быть как раздельным, так и в совокупности.

События вокруг Украины лишний раз подтвердили, что в условиях, когда речь идет о базовых интересах западных стран, используется тот вариант силы, с помощью которого можно получить максимальный результат и который способен привести к поставленной цели независимо от этической стороны предпринятых действий.

Отношение к «мягкой силе» в российском политическом руководстве неоднозначное. С одной стороны, отдается должное «мягкой силе» как комплексному инструментарию для решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии, с другой стороны, высказываются опасения, что «усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам подчас деструктивного и противоправного использования «мягкой силы» и правозащитных концепций в целях оказания политического давления на суверенные государства, вмешательства в их внутренние дела, дестабилизации там обстановки, манипулирования общественным мнением и сознанием, в том числе в рамках финансирования гуманитарных проектов и проектов, связанных с защитой прав человека, за рубежом» (Концепция внешней политики Российской Федерации от 12 февраля 2013 г.).

Все большее значение в арсенале «мягкой силы» имеют средства и методы воздействия, в основе которых лежит коммуникация. На уровне государств эти методы объединены в информационную политику, характер которой в полной мере свидетельствует о ценностных ориентирах и предпочитаемых способах достижения поставленных целей, свойственных данному политическому режиму и обществу в целом.

В 2007 году в России создан некоммерческий фонд «Институт демократии и сотрудничества» (европейское представительство находится в Париже, возглавляет Н.А. Нарочницкая, нью-йоркское представительство возглавляет А.М. Мигранян). Миссия института — служить «мостом» между Россией и иностранными государствами, быть местом для диалога общественных организаций с той и другой стороны, местом пересечения информационных потоков и налаживания связей.

Среди наиболее эффективно действующих СМИ, работающих на внешнюю аудиторию, является RT (Russia Today) - российская международная многоязычная информационная телевизионная компания. Russia Today – первый англоязычный информационный канал, представляющий российскую точку зрения на события, происходящие в России и за рубежом.

Её основной англоязычный канал RT International — первый российский информационный телеканал, ведущий круглосуточное вещание на английском языке. RT — это три круглосуточных информационных телеканала, вещающие из Москвы более чем в 100 странах мира на английском, арабском и испанском языках, телеканалы RT America и RT UK, выходящие в эфир из собственных студий в Вашингтоне и в Лондоне, документальный канал RTД, а также глобальное новостное видеоагентство RUPTLY, предлагающее эксклюзивные материалы телеканалам всего мира.

В условиях жесткого информационного противодействия использование различных информационных каналов на формирование альтернативной Западу точки зрения является не только оправданной, но и необходимой формой защиты национальных интересов России.

Блохина М.Ю.
Россия, Санкт-Петербург, Университет ИТМО

ИСПОЛЬЗОВАНИЕ ОБРАТНОГО ПРОЕКТИРОВАНИЯ В РАМКАХ МОДЕРНИЗЩАЦИИ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Своевременное информационно-аналитическое обеспечение исполнительных органов государственной власти обусловлено высоким уровнем ответственности за принимаемые решения, сложностью исполнения поставленных задач и необходимостью оперативно принимать решения в условиях резкого изменения обстановки в регионе. Высокие темпы разработки системы поддержки принятия решений для органов государственной власти способствовали запуску рабочей версии информационно-аналитической системы в короткие сроки. Кроме того, внедрение аналитической системы способствует решению таких задач, как: сбор и обработка данных из различных источников, консолидация, представление, моделирование и прогнозирование, обеспечение конечного пользователя аналитическим материалом в контексте показателей социально-экономического становления субъекта. Модернизация и развитие системы поддержки принятия решений в условиях стремительного развития информационных технологий, появления новых источников информации и политики импортозамещения, становятся актуальной задачей.

Целью исследования является совершенствование существующих бизнес-процессов системы поддержки принятия решений для обеспечения деятельности органов государственной власти.

Процесс совершенствования разработанной информационной системы неразрывно связан с использованием метода обратного проектирования или реверс-инжиниринга – построением моделей на основе существующего кода. Этот метод позволяет построить информационную модель существующей системы, модификация которой, позволит усовершенствовать бизнес-процессы исходной системы поддержки принятия решений. Одним из видов обратного (реверс) инжиниринга является трансформация информационной системы, с целью улучшения структуры, без изменения сценариев поведения, для модернизации возможностей, расширения функциональной составляющей системы. Инструментальным для построения информационной модели выбран унифицированный язык моделирования (UML). Графическое построение существующей модели позволит визуализировать элементы аналитической системы, с помощью схем, однозначно интерпретируемых специалистами разного профиля.

Как и прямое так и обратное проектирования инициируется созданием концептуальной модели, для ее построения в нотации UML строится диаграмма-прецедентов, диаграмма видов деятельности и диаграмма последовательностей. Следующий этап – построение логической модели из физической модели данных. Логическая модель данных представлена в виде диаграммы классов, на основе диаграмм последовательностей и диаграмм состояний.

При выборе подхода к обратному проектированию системы поддержки принятия решений, следует учитывать, что графические схемы широко используются при управлении проектированием масштабных систем высокой сложности, которыми являются системы поддержки принятия решений для обеспечения деятельности органов государственной власти. Визуальные модели являются наиболее приспособленными для решения задач, которые возникают при создании информационных систем. Создание моделей графических элементов системы и их визуализация способствует взаимопониманию между заказчиками и исполнителями, обеспечивает прозрачность и обоснованность выбранных архитектурных решений и, наконец, позволяет понять какой будет модернизированная аналитическая система.

Лепёхин А.Н.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь

О ФОРМИРОВАНИИ МЕТОДОЛОГИЧЕСКИХ ОСНОВ ПРИ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Современные реалии управленческой деятельности характеризуются необходимостью формирования новых подходов к организации информационного и аналитического обеспечения управления различными социально-экономическими процессами и системами.

Информационное обеспечение государственного управления на современном этапе активно развивается. Так, в Республике Беларусь еспублики настоящее время уже разработаны и внедрены большое количество баз и банков данных, обслуживаемых различными государственными органами. Кроме того, для решения правоохранительных задач активно используются информационные массивы и негосударственных предприятий и организаций. Объективно указанные информационные потоки налагают определенные требования к организации работы с большими объемами информации и обуславливают необходимость выделения системы принципов информационно-аналитического обеспечения правоохранительной деятельности.

С развитием информационных технологий значение информационно-аналитического обеспечения неуклонно возрастает. В настоящее время к организации информационно-аналитического обеспечения деятельности правоохранительных органов и качеству аналитической

работы в условиях происходящих процессов информатизации общества и формирования в государстве единого информационного пространства предъявляются новые повышенные требования.

В этой связи теоретические аспекты формирования методологических основ информационно-аналитической работы обусловливают необходимость упорядочения системы принципов организации такой деятельности. В этой связи, очевидно, что помимо основных общеотраслевых принципов, определяющих основные направления осуществления и развития информационно-аналитического обеспечения правоохранительной деятельности, которые включают в себя принципы – законности, соблюдения прав и свобод граждан, сочетания гласных и негласных форм и методов работы, а также экономичности осуществляемой деятельности, можно выделить ряд специальных принципов рассматриваемой деятельности. К ним следует отнести следующие принципы.

1. Правовой регламентации информационных процессов, что обусловлено с одной стороны необходимостью соблюдения требований законности осуществляемой деятельности, с другой стороны, коррелирующей с первым требованием, последующей возможностью использования собираемой информации не только в оперативно-розыскных целях, но и использования ее в уголовном судопроизводстве.

2. Оперативности и информационной емкости информационно-аналитического обеспечения деятельности правоохранительного органа – что предполагает с одной стороны, предоставление информации, имеющей значение лицу принимающему решение (ЛПР), в максимально короткие сроки, с другой, речь должна идти не только об информировании ЛПР о каких-либо фактах и событиях, но и предоставление аналитической информации (справки, отчета), отражающей причины и факторы, способствующие тому или иному развитию событий, возможные последствия и прогнозное развитие ситуации, и, при необходимости, предложения по разрешению ситуаций.

3. Организационной упорядоченности и единства источников обработки информации – что предполагает создание единых центров обработки информации в рамках правоохранительных органов и четкую организационно-правовую регламентацию их деятельности, включающую наделение их функциональными обязанностями и правами по сбору в рамках всех подразделений органа всей необходимой информации для решения возложенных задач, ее обработке, хранении и использовании для решения задач информационно-аналитического обеспечения в рамках выполнения функций, возложенных на правоохранительный орган.

4. Полноты и достоверности собираемой информации – что направлено на максимальный охват, как по количеству источников информации, так и использование максимально достоверной собираемой информации (с применением системы весовых коэфицентов источников информации).

5. Научности используемых сил, средств и методов информационно-аналитической работы – что направлено в первую очередь на получение качественного аналитического продукта – отчета, справки, прогноза, и предполагает, использование различных математических методов и моделей, специализированного программного обеспечения по обработке информации и формировании отчетов и подготовленного персонала, эффективно решающего задачи информационно-аналитического обеспечения деятельности правоохранительного органа.

Очевидно, что приведенный перечень принципов информационно-аналитического обеспечения не является исчерпывающим, и, как полагаем, будет расширен в ходе научных исследований, проводимых, как автором, так и другими исследователями.

Бурлов В.Г., МокееваТ.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макаров

РАЗРАБОТКА ДИНАМИЧЕСКОЙ МОДЕЛИ УПРАВЛЕНИЯ В СОЦИАЛЬНОЙ И ЭКОНОМИЧЕСКОЙ СИСТЕМЕ

Для разработки информационно-аналитического обеспечения в интересах органов государственной власти необходимо создание модели управления.

В условиях кризиса для корректного управления территориями, создаются системы управления. Как известно из системотехники, существует только два подхода разработки системы

- на основе анализа
- на основе синтеза.

При выборе подхода на основе анализа (решение проблемы выбора) выдается набор физических элементов и требуется предсказать возможный результат функционирования системы (некоторые выходные характеристики). То есть необходимо сформировать отдельно несколько вариантов развития ситуации. Проанализировав результат функционирования каждого, выбирается тот вариант, результат которого максимально приближен заявленным требованиям.

При разработке на основе синтеза выдается набор выходных характеристик проектируемой системы, и требуют определить количественный и качественный состав системы. То есть при анализе решается задача «от начала» и анализируется, что получится. При синтезе решается задача «от конца», желаемого результата; формируется система с требуемыми выходными

характеристиками. Для разработки системы на основе синтеза необходимо знать закон построения и функционирования системы.

В настоящее время в основном аппарат создается на основе анализа, который не позволяет получить гарантированный результат. В синтезированной модели разработчик имеет возможность формировать процессы с наперёд заданными свойствами и учитывать в формализованном виде характерные предметной области закономерности.

Управление субъектом, как любое другое управление, осуществляется на основе результатов моделирования процессов социально-экономического развития субъекта в рамках выбранной концепции управления. Модель - это система, исследование которой служит средством для получения информации о другой системе.

Системообразующей основой динамической модели является система дифференциальных уравнений, описывающая изменения 3-х основных системообразующих показателей: показатель численности населения Субъекта, показатель экономического развития субъекта, показатель энергообеспеченности Субъекта. (Обобщённый индекс развития промышленного производства).

Через 9 введенных коэффициентов системы дифференциальных уравнений проявляются механизмы реализации региональной политики в интересах достижения цели государственного управления. Эти коэффициенты представляют собой: коэффициент демографической активности; коэффициент антимотивации людей к деторождению; коэффициент обеспеченности Субъекта энергией; коэффициент заинтересованности людей в развитии экономики; коэффициент развития реального сектора экономики; коэффициент энергообеспеченности рабочих мест; коэффициент развития энергообеспеченности Субъекта; коэффициент соответствия населения энергообеспеченности; коэффициент соответствия развития экономики энергообеспеченности.

Практическая ценность определяется возможностями методологии синтеза модели процесса управления в социальной и экономической системе и заключается в том, что полученная модель позволяет: вырабатывать концепцию управления системами, действующих в интересах обеспечения жизнедеятельности региона; формировать исходные данные для выработки ЛПР замысла планов действия и порядка принятия решений; разрабатывать системы поддержки принятия решения; реализовать технологию управления жизнедеятельностью региона; повышать оперативность управления социальными и экономическими системами; повышать качество принимаемых решений по оперативному и организационно-техническому управлению.

Разработанная методология статического управления позволяет по новому поставить задачу государственного управления как отдельным Субъектом, так и страной в целом. При практической реализации модели задача органов государственного управления сводится к формированию девяти коэффициентов и обеспечение достижения цели управления путем различных управленческих решений и действии. При создании ситуационного центра на основе данной модели результат работы будет гарантированным.

Чикунов В.В.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь

О ПОНЯТИИ И СОДЕРЖАНИИ ИНФОРМАЦИИ В КОНТЕКСТЕ ПРОВЕДЕНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Современное социально-экономическое и политическое развитие с начала XXI в. свидетельствует об упрочнении государственности и правопорядка в стране, о развитии демократии и самоуправления в обществе. Дальнейшая реализация курса на достижение политических идеалов, экономического роста и повышения личного благосостояния граждан возможна при минимизации внешних и внутренних угроз, активном противодействии проявлениям преступности, совершенствовании работы всех государственных институтов, включая правоохранительные органы.

Вместе с тем, сложность и неоднозначность процессов, протекающих в мире, риски стремление получить хороший результат, многообразие и избыточность информации, необходимость ее селекционирования, отсутствие достоверного знания заставляют применять информационно-аналитическую деятельность в повседневной жизни, она становится важнейшей характеристикой современного общества.

Следует отметить, что научное понятие информации охватывает чрезвычайно широкие многообразия взаимосвязанных, взаимообусловленных и взаимозависимых материальных объектов и мыслительных процессов. Отсюда возникают сложности в его однозначном определении. В соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации»: «Информация - это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Рассматривая понятие «оперативная информация» («оперативно-розыскная информация»), отметим, что оно имеет уже более чем полувековую историю. В настоящее время научной литературе определяется как сведения о лицах (сообществах физических лиц), предметах, документах, фактах, событиях, явлениях и процессах, получаемые в порядке, предусмотренном

оперативно-розыскным законом и ведомственными нормативными актами по тактике оперативной деятельности, зафиксированные на материальных носителях с реквизитами, позволяющими ее идентифицировать, сосредотачиваемая в информационных системах и делах оперативного учета. Данная информация образует информационный ресурс оперативных подразделений органов, осуществляющих оперативную деятельность, отличающийся конфиденциальным характером. Информация, циркулирующая в оперативно-розыскном процессе, призвана обеспечить решение задач оперативной деятельности, содействовать разрешению стоящих проблем. В основе названия «оперативная информация» лежит способ ее производства – оперативная деятельность. Уточнение «оперативная информация» – это не содержательная, а производственная характеристика информации, которая подчеркивает, что это не просто «сведения о…», но «сведения о…», полученные соответствующим образом, в нашем случае – оперативным способом.

Содержание оперативной информации отличается широким разнообразием сведений, относящихся также и к характеристике различных сторон оперативной обстановки, основных сил оперативной деятельности, оценке результатов их использования. Оперативная информация отражает широкий круг явлений, обстоятельств, событий, имеющих непосредственное или потенциальное значение для планирования и осуществления оперативно-розыскных мероприятий, проведения оперативно-аналитической работы. Вышеприведенное определение позволяет выделить специфичные признаки информации:

Во-первых, в ходе оперативной деятельности собираются сведения о конкретных объектах;

Во-вторых, для того чтобы информация приобрела соответствующий правовой статус, она должна получаться только на законных основаниях и с соблюдением установленных для этого условий;

В-третьих, анализируемая информация подлежит фиксации на материальных носителях, в частности отражаться в оперативно-служебных документах, иметь материальную форму При этом материальные (физические) носители информации и различного рода оперативно-служебные документы призваны обеспечивать формирование информационного ресурса органа, осуществляющего оперативную деятельность;

В-четвертых, оперативная информация имеет в основном конфиденциальный характер, в связи с чем, доступ к ней ограничивается в соответствии с законодательством, и устанавливается порядок ее использования в рамках уголовного или административного процесса и иных видов правоохранительной деятельности;

В-пятых, оперативная информация предназначена для решения не только задач, установленных для оперативной деятельности и обязанностей, возложенных на конкретные оперативные подразделения органов, осуществляющих ОРД, но и задач уголовного процесса и других видов правоохранительной деятельности.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Глебов Н.Б., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК УГРОЗА БЕЗОПАСНОСТИ ОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ В ОРГАНИЗАЦИИ

В повседневной практики, когда идет речь о безопасности IT-инфраструктуры организации, а именно корпоративных сетей передачи данных, первое, что приходит на ум – это вредоносный код, который атакует ресурсы сетей. Например, он атаковал ядерные объекты Ирана в 2009-2010 годах и вывел из строя завод по обогащению урана, но котором центрифуги, которые обогащали уран, были выведены из строя специально подготовленным вредоносным кодом. Этот случай официально считается первым случаем такого масштаба. На самом деле это далеко не первый случай: и до этого были атаки на различные объекты, в том числе на атомные электростанции и после этого были различные атаки, например, в 2014 году такая атака была успешно реализована на одно из сталелитейных предприятий Германии. Явных подтверждений в прессе Вы не увидите, но факты свидетельствуют о том, что использующийся вредоносный код вывел из строя ряд физически активных и задействованных в технологическом процессе объектов этого завода.

Опорные точки реализации угрозы:

- Манипуляция в автоматизированной системе управления технологическими процессами, предотвратившая отключение доменной печи;
- Доступ в индустриальный сегмент через бизнес сеть;
- Доступ в бизнес-сеть через узконаправленный фишинг;
- Компрометация множества систем: это привело к невозможности отключения;
- Злоумышленник обладал высокой квалификацией и знанием по атакуемой системе.

Обратим внимание на «узловое» звено цепи – узконаправленный фишинг. Именно этот метод позволил получить доступ к ресурсам рассматриваемой сети.

Фишинг - это лишь один из методов популярной в наше время области - социальная инженерия – методы получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Именно в борьбе и противодействии методам социальной инженерии и должен делаться акцент при обеспечение безопасности современной сети передачи данных в организациях разного уровня: от небольшой офисной фирмы, до крупного предприятия.

Глебов Н.Б., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Социальная инженерия – методы получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

О том насколько учет этих методов важен при обеспечении безопасности сетей передачи данных и процессов на предприятии речь шла в предыдущей статье.

Здесь мы остановимся лишь на обзоре основных методов социальной инженерии:

Претекстинг - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.

Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей - авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма

для ввода персональных данных (пин-кодов, логина и пароля и т.п) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

Кви про кво (услуга за услугу) – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Обратная социальная инженерия - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Забарин А.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД РФ

МАССОВЫЕ БЕСПОРЯДКИ КАК КОГНИТИВНЫЕ ТЕХНОЛОГИИ СЕТЕВЫХ ВОЙН

Бурное развитие и доступность информационных технологий перевели процесс функционирования неформальных и формальных сетей общения в цифровую форму, и есть тенденция к тому, что эта форма вскоре станет определяющей. У участников сетей есть собственное отношение как к своей стране и ее властям, так и к другим странам и властям, и на это отношение можно влиять. Настраиваемый интерфейс площадки виртуального общения, топ новостей, новости друзей, групп, работа модераторов, комментарии, политика блокирования блогов и др. – все это инструменты менеджмента восприятия в отношении соответствующих событий.

Сетевая война представляет собой борьбу за навязывание участникам реальных или виртуальных сетей общения своей картины мира, своего понимания событий, своих смыслов, потребностей, мотивов, ценностей. Войны крайне редко ведутся за прямое физическое уничтожение противника. В основе войн лежит разное представление о соотношении позиций субъектов конфликта в будущем. Условно говоря, если мирное население будет с нетерпением ждать, когда же армия противника «освободит его от ненавистного тирана» и обеспечит ему изобилие и процветание, война теряет всякий смысл. Когнитивные технологии направлены на формирование в сознание населения противника установки на приемлемость, оправданность и желательность подобной предательской позиции.

На примере оранжевых революций мы видим управляемую стихию массовых беспорядков, посредством которой происходит захват власти. Традиционные массовые беспорядки выражались в насильственных действиях толпы. Когнитивные технологии трансформировали их в модель ненасильственных действий. Коллизию о том, определяется ли общественный порядок нормами права или общественным мнением стали разрешать в пользу общественного мнения: «Государство погрязло в коррупции – это проявление общественного беспорядка, а свержение власти коррупционеров – это наведение общественного порядка».

Другой целью когнитивных технологий стала деформация представлений о самом порядке. Беспорядки существуют там, где есть четкое представление о том, что такое порядок. Там, где нет уважения к законам, где закон не понятен гражданину и дискредитирован практикой правоприменения, где социальные нормы размыты, где нарушение норм – не исключение, а правило, где нельзя определить правого и виновного, там исчезают отличия и порядка от беспорядка. Когда в сознании населения противника исчезают критерии того, что такое норма или вводится множество

взаимоисключающих критериев нормы, то соответственно разрушается граница и между нормами и их нарушением, порядком и беспорядком.

Когнитивная сфера, национальные ценности, традиции, нормы должны стать объектом особой охраны для обеспечения информационно-психологической безопасности России.

Работа выполнена за счет средств федерального бюджета, выделяемых РГНФ № 8.16.433.2014.

Кефели И.Ф.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ИДЕОЛОГЕМА «РУССКИЙ МИР» В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОМ ПРОТИВОБОРСТВЕ

При рассмотрении Русского мира в культурно-историческом и геополитическом контексте необходимо обратить внимание, в первую очередь, на следующие его характеристики:

- Русский мир предстает культурно-исторической общностью этносов и населяемых ими территорий, находящихся под влиянием российской культуры и государственности;
- Русский мир следует представлять как политический лозунг, отражающий имперские настроения, а после возврата Крыма в Россию – ключевое звено внешнеполитической доктрины России;
- Русский мир выступает «цивилизационным пространством», покоящимся на православии, русской культуре и общей исторической памяти;
- Русский мир следует рассматривать как одну из геоцивилизаций полицентричного мира и как актор геополитики – глобальной по масштабам и информационной по своему проявлению.

Такое многообразие толкований Русского мира «свертывается» в идеологему (греч. idéa – понятие и agein – вести) «Русский мир», которая рассматривается как один из элементов идеологии, ключевая мысль, претендующая на наиболее полное и достоверное выражение содержания общественного сознания.

Из данного суждения следует, что данная идеологема оказывается в эпицентре информационно-психологического противоборства, поскольку в ней преобладает положительный, жизнеутверждающий аксиологический модус – Родина, Отечество, справедливость (в отличие от негативного аксиологического модуса – террор, война, несправедливость). Психологическую уязвимость идеологемы «Русский мир» следует объяснить тем, что она заключает в себе также элементы смешанного аксиологического модуса (патриотизм, демократия, народ), оценочный потенциал которого допускает порой противоположное толкование одних и тех же событий, действие, поступков.

В международной практике сегодня это достаточно четко можно проследить в действиях американской администрации, манипулирующей исключительно в своих интересах понятием «умеренная оппозиция» в Сирии.

В условиях глобальной трансформации мироустройства и перемещения России на «западный фланг формирующейся Большой Евразии» вопрос о месте и роли Русского мира в пространстве евразийской интеграции следует анализировать и решать, прибегая к законам геополитики, учитывая приобретение ею, геополитикой, нового качества – информационной геополитики. Последняя утверждает, что судьба пространственных отношений между государствами все более определяется превосходством в киберпространстве, а в информационном противоборстве деформируется главный геополитический потенциал государства – символический капитал культуры. Здесь будет весьма уместным прибегнуть к диалектике, закону отрицания отрицания: спустя поколение, мы все чаще начинаем обращаться к советскому опыту, образу жизни, культуре, которые отвергались в 1990-е годы, а спустя четверть века возвращаются к нам в виде актуализированной идеологемы «Русский мир».

В советское время Русский мир представлял собой «плоть и дух» отечественной культуры – национальной по форме, социалистической по содержанию и восприемницей всего культурного наследия народов нашей многонациональной страны. Ныне Русский мир – это некая Атлантида, память о великом прошлом и, вместе с тем, реальная данность, воссоздаваемый образец культуры, который должен выступить объединяющим началом не по своей воле разделенных по национальным квартирам народов.

Такова задача идеологов и ревнителей Русского мира. На уровне стратегического планирования идеологема «Русский мир» должна быть взята на вооружение как средство противодействия манипуляции массовым сознанием. На фоне заката «Большой Европы» и зарождения «Большой Евразии» идея Русского мира становится особо привлекательной, хотя в условиях расширения фронта информационно-психологической войны – подвергаемой политическому и идеологическому подавлению.

Колотов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ТЕХНОЛОГИИ ВЕДЕНИЯ ГИБРИДНЫХ ВОЙН НА ДАЛЬНЕМ ВОСТОКЕ В ИСТОРИЧЕСКОЙ РЕТРОСПЕКТИВЕ

Мудрецы Древнего Китая ещё в VI в. до н.э. обращали внимание правителей на то, что «сто раз сразиться и сто раз победить – это не лучшее из лучшего; лучшее из лучшего – покорить чужую армию не сражаясь» (Сунь-цзы. Искусство войны / пер. Н. И. Конрад // Искусство войны: Антология военной мысли. — СПб.: Амфора, 2009. С. 20.). Стратег и полководец Сунь-цзы в своём знаменитом трактате «Искусство войны» писал: «Самая лучшая война – разбить замыслы противника. На следующем месте – разбить его союзы. На следующем месте – разбить его войска. Самое худшее – осаждать крепости». На древнекитайском языке в данной цитате в порядке убывания приоритетности употреблены следующие объекты воздействия: 謀 móu (замыслы), 交 jiāo (отношения), 兵 bīng (войска), 城 chéng (крепости). Если сопоставить термины времён Сунь-цзы и современные нам категории, то получается, что уже в то время правильной считалась именно гибридная война, которая состояла из двух составляющих информационной воны: когнитивное оружие и дипломатическая деятельность. Только две последние категории относятся к ведению традиционных военных действий (битвы между армиями и штурм городов). При этом сугубо военные элементы по Сунь-цзы имеют вторичное значение. Отсюда получается лаконичный вывод: «Поэтому тот, кто умеет вести войну, покоряет чужую армию, не сражаясь; берет чужие крепости не осаждая; сокрушает чужое государство, не держа своё войско долго». При этом все время следует помнить главную мысль древнего трактата, которая имеет столь актуальное и в наши дни звучание «Война – это путь обмана».

Взяв на вооружение изложенные ещё в глубокой древности принципы, в середине XX века вьетнамский национальный лидер Хо Ши Мин их творчески переработал для того, чтобы сразиться с одной из самых современных колониальных армий того времени – французским экспедиционным корпусом, который опирался на подавляющее превосходство в военной и технической мощи. Вьетнамцы могли опираться только на единственный доступный им ресурс – стратегическое планирование, которое в старое время именовалось «замыслами» и противопоставить древние стратагемы подавляющему техническому превосходству противника.

Хорошо известно, что Вьетнам победил в Первой Индокитайской войне (1946-1954), но подробное описание стратегических замыслов и их реализация противоборствующими сторонами до сих пор мало известны широкой публике. Данный доклад ставит своей целью восполнить этот пробел и на конкретных примерах показать как информационные технологии глубокой древности помогли победить вооружённую современным оружием европейскую армию на индокитайском театре военных действий.

Комлева Н.А.
Россия, Екатеринбург, Центр геополитического анализа

ИДЕОЛОГИЧЕСКАЯ ГРАНИЦА КАК ПРЕДЕЛ БЕЗОПАСНОСТИ ИДЕОЛОГИЧЕСКОГО ПРОСТРАНСТВА

В таком случае идеологическая граница общества – это степень допустимого проникновения в его идеологическое пространство. Допустимым же проникновением является воздействие на массовое сознание данного общества оформленных теоретических концептов или дисперсных форм ценностей другого общества, не разрушающее существующую в данном обществе систему ментальных ценностей. Разрушительное воздействие, тем более имеющее целенаправленный характер, представляет собой информационно-идеологическую агрессию, т.е. акт войны. В любой системе, в том числе в системе ментальных ценностей, существуют ключевые элементы, «краеугольные камни», разрушение которых является фатальным для системы в целом. Информационно-идеологическая агрессия (война) направлена именно на ликвидацию и замещение базовых ментальных ценностей общества-противника как «краеугольных камней» структуры его идеологического пространства. Думается, что ключевых точек идеологического пространства не так уж много. Это прежде всего признание ценности семьи, почитание предков (одобрение генерального хода истории данного общества), уважение к государству и его официальной идеологии, догматы доминантной религии. Совокупность ментальных приоритетов массового сознания и составляет идеологическую границу общества. Указанные ценности, сложенные в систему, предопределяют устойчивость общества к испытаниям, его ментальную выживаемость, поскольку именно они обеспечивают адекватную социальную самоидентификацию как на уровне массового, так и на уровне индивидуального сознания. Важность ментальных приоритетов, или ментальной доминанты, состоит в том, что они определяют форму и степень осознания национального интереса как обществом в целом, так и его политической элитой. Временная утрата ментальной доминанты ведет к геополитической дезориентации общества до момента обретения им другой доминанты и может явиться одной из причин геополитического сжатия данного государства. Ментальные ресурсы – это то

самое «пространственное чувство» народа, без развития которого не может осуществляться геополитическая экспансия.

Идеологическая граница общества не тождественна идеологической границе государства.

Идеологическая граница государства, по нашему мнению, это совокупность ментальных приоритетов массового сознания, обеспечивающих поддержку большинства избирателей в процессе формирования выборных органов государственной власти и лояльность подвластных ко всем трем ветвям государственной власти в период между выборами.

Информационно-психологические войны велись на протяжении всего XX века, но с приходом к власти в США президента Р. Рейгана информационно-идеологическое воздействие стало принципиально иным: началась эра глобальной борьбы за сознание целых народов с использованием новейших информационно-психологических технологий на основе координации деятельности всех государственных структур и спецслужб США. При Рейгане государственные органы стали в возрастающей степени использоваться в качестве координационных и направляющих центров информационно-психологического воздействия. Центральную роль в процессе стратегического анализа и координации деятельности информационно-психологических структур США приобрел Совет национальной безопасности. Во второй половине XX века с активным развертыванием информационной революции стало очевидным, что именно информационные (идеологические) воздействия способны изменить главный геополитический потенциал государства: национальный менталитет, культуру и моральное состояние людей. Тем самым вопрос о роли символического капитала в геополитическом процессе приобрел стратегическое значение. Национальная психология в современном мире может незаметным для нации образом изменяться ее геополитическими противниками. Итак, со времени 80-х годов XX века задача защиты идеологических границ государства и общества выходит на передний план в структуре деятельности по обеспечению национальной безопасности.

Защита идеологической границы, в отличие от защиты границы географической, является исключительной функцией элиты: как элиты политической, так и элит в сфере науки, культуры и образования. Угрозы для ментальной безопасности общества и государства могут быть осознаны только на уровне социальных групп, обладающих для этого соответствующими знаниями и квалификацией.

Мельник Г.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ТАКТИЧЕСКИЕ МЕДИА КАК УГРОЗА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

В последнее десятилетие усилился интерес медиаисследователей к изучению тактических медиа (tactical media), представляющих собой информационные ресурсы, используемые субъектами сетевой коммуникации для побуждения к политическим действиям протестного характера и приведения в активное состояние политической системы для достижения какой-либо разрушительной задачи в реальной борьбе, чаще всего направленной против государственной политики.

Рассмотрение деятельности тактических медиа в связи с проблемой информационнно-психологической безопасности объясняется тем, что этот корпус новых медиа позиционирует себя как исключительно радикальный и оппозиционный, направленный на критику политического режима.

В целеполагании функционирования этого корпуса СМИ заложены идеи расслоения общества, разрушения глобальных социальных структур. Программные документы Tactical media (TT) неизменно декларируют необходимость борьбы «с устойчивой тенденцией к репрессиям, эксплуатации, изоляции, отчуждениями и корпоратизацией». Нередко ТТ маркируют себя как «медиа кризиса, критики и оппозиции». Информационная деятельность тактических медиа имеет продолжение в радикальных акциях, митингах, уличных беспорядках, которые могут длиться несколько дней. Выражение виртуального протеста в Интернет перетекает в ритуальные действия с непременной декламаций, лозунгами, символикой и отрежиссированными столкновениями с полицией.

Тактические медиа, претендующие на общественный контроль за действиями власти, меняют конфигурацию классической политики, подрывая нормативную властную систему информационными атаками. Используя стратегии и техники продвижения в аудитории политических идей протеста, инакомыслия и бунта, программ, символов, тактические медиа мобилизуют аудитории на проведение небезопасных социальных перфоменсов и политических флэшмобов («Оккупай Абай» и др.) Уже сами названия изданий несут в себе энергетический заряд («Наперекор», «Община», «Прямое действие», «Свобода или смерть», «Новый Свет», «Петроградец», «Намерение», «Удар», «Тротиловый эквивалент», «МедиаУдар») и указывают на их подрывную деятельность. «Достверность» отображаемых событий достигается публикацией множества фотографий и скан-копий документов, видеозаписей в оперативном режиме. Международные информационные платформы «МедиаУдар», IndyVideo не только публикуют записи акций, но и обучают всех желающих пользоваться камерой и монтировать видео. Нередко эти медиа выступают средством координации действий в организации «умных толп» против глобальных организаций (G8, G20, WTO) и корпораций

(Microsoft, Pepsi, Nike и др.). Тактические медиа стали структурным информационным компонентом в таких важных политических процессах, как пробуждение радикального ислама, парад «цветных революций», порождение арабской весны и «майданов". Как коллективный актор медиа в этих процессах с успехом реализовали функции мобилизации, подрыва, разрушения. Локальные по месту образования, тактические медиа становятся глобальными по воздействию, создавая сети активистов, позволяющих ускорять распространение опробованных техник и влиять на политические ситуации.

Таким образом, тактические медиа выступают как эффективный информационный, идеологический, мобилизационный, организационный и синхронизирующий ресурс, где аккумулируются разрушительные идеи и формируется база оппозиционных коммуникативных практик, где быстро достигаются политические задачи при ограниченных временных, финансовых и эмоциональных затратах.

Информационно-психологическая угроза безопасности тактических медиа заключается в том, что они без меры расширяют критическое пространство, увеличивают степень конфликтогенности политического взаимодействия в условиях глобализации, ориентируют социум на деструктивные (дестабилизация, дезорганизация, дезинтеграция) действия.

Плебанек О.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф.Устинова

КОГНИТИВНО-АКСИОЛОГИЧЕСКИЕ МЕХАНИЗМЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

1. Информационные и гибридные войны, «цветные революции» в различных ставят вопрос о противодействии информационно-когнитивным технологиям. В современных условиях достижение информационной закрытости общества не представляется возможным, поэтому единственным надежным средством противодействия программирующему воздействию возможного противника является консолидация общества вокруг идеологии, противостоящей деструктивному воздействию недружественных сторон.

2. Идеология представляет собой рациональный уровень восприятия действительности, и поэтому является необходимым, но недостаточным элементом системы противодействия информационному противнику. Национальная идея представляет собой эмоционально-мотивационный механизм программирования социальной деятельности на иррациональном уровне. Национальная идея на символическом уровне имеет идеологемную экспликацию. Идеологема как когнитивная единица идеологии в силу своей лаконичности и упрощенности быстрее достигает сознания адресата и ориентирована на самый широкий адресный круг, независимо от возраста, уровня образования, этнической и религиозной принадлежности индивидуума.

3. В связи с этим в цели социального конструирования должны входить следующие задачи:

– разработка идеологем-понятий, идеологем-фреймов, идеологем-гештальтов, отражающих идеологию государства, как положительного (Родина, гуманизм), так и отрицательного аксиологического модуса (терроризм, геноцид)

– вытеснение из СМИ (из системы образования) идеологем со смешанным аксиологическим модусом (воля, личность, конкуренция)

– нейтрализация идеологем ограниченного употребления, конституирующих деструктивную идеологию (чеченский борец за независимость, советский оккупант)

– формирование цепочек идеологем-историзмов, конституирующих осознание цивилизационной преемственности (русская идея, светлое будущее, геополитическое равновесие)

Попов П.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова

ИДЕОЛОГЕМА КАК ЭЛЕМЕНТ ГИБРИДНОЙ ВОЙНЫ

Мы живём в состоянии войны. Войны, которая не прекращалась. В настоящее время она носит название гибридной, поскольку на начальном этапе в ход идут не вооруженные силы, а информационные, политические, финансовые технологии.

Целями ведущейся информационной войны против любой страны, отстаивающей собственный суверенитет, в том числе является максимальная дезориентация и разрушение ценностей противостоящей стороны, подчинение ресурсов для использования в собственных интересах.

Одним из инструментов разрушения является использование эмоционально окрашенного политического термина, элемента идеологической системы, как идеологема. При этом значение идеологемы меняется в соответствии с политической конъюнктурой. Целенаправленное использование идеологем является эффективным средством управления массовым сознанием, она легко запоминается и создает иллюзию понимания у объекта манипуляции.

Такие формально позитивно маркированные идеологемы, как «общечеловеческие ценности», «либерализация», «демократия», «новое мышление» отражают определенные политические взгляды, способствуют идеологическому воздействию на адресата. Идеологемы называют «оружиями лжи и обмана», но лгут и обманывают не слова, а авторы политических текстов.

Идеологемы всегда тесно связаны с политическим контекстом, т.к. с их помощью давалось идеологическое обоснование «новой стратегии» во внешней и внутренней политике. Хотя формально декларировался отказ не только от прежней идеологии, но и от идеологии вообще.

Однако, при заимствовании ценностей вместе с понятиями из другого языка, другого образа мира, собственные ценности утрачивают свою ясность, а с помощью привнесенных ценностей государствами и людьми неизбежно пытаются управлять те, кто навязал их извне.

В современной цивилизации господствует транснациональный капитал, существующий ради извлечения прибыли. Для бесконечного роста нужен потребитель, который может (должен) постоянно приобретать «материальные блага». Такому порядку ранее обычно препятствовали образование и культура, с их знаниями, ценностями и этическими правилами. Образованный человек, встроенный в культуру своего народа, имеет и свои культурные ограничения. Если есть эти соблюдаемые человеком самоограничения – можно вести речь о человеке, его свободе и ответственности, о народе. Нет самоограничения – перед нами лишь потребитель, масса, нечто аморфное.

Другой момент, связанный с деструктивной деятельности капитала состоит в необходимости большого количества дешевой рабочей силы. Один из вариантов решения - наличие множества низкооплачиваемых «гастарбайтеров», представителей других культур и народов, что неизбежно влияет на политическую и культурную системы страны, как единого организма. Для снятия возможных внутренних конфликтов государству навязываются идеологемы «толерантности», «политкорректности» и т.д., разлагающие единую социокультурную систему общества.

Подмена понятий стала оружием для разрушения ценностей и духовно-нравственных основ России. Разрушители называются «реформаторами», мошенники «бизнесменами». Продажу природных ресурсов называют «экономикой», а сокрытие доходов и их вывод за границу - словом «офшор». Можно встретить утверждения, что борьба с экономическими преступлениями и взятками - это диктатура, и наоборот, развал власти и безответственность - это демократия.

В настоящее время многим становится понятно, что в навязанной идеологеме «общечеловеческие ценности» присутствуют явные несоответствия реальности:

– ценности в каждой из культур являются если и не уникальными, то отличающимися или особенными;

– западная цивилизация под такими ценностями понимает «материальные блага», «деньги», «доход», «прибыль».

При этом эффективность геополитики, проводимой нашими «стратегическими партнерами» кроется за туманом бессмысленных абстрактных и высокопарных фраз и достаточно проста - обман, коварство и подлость. Готовность всё ещё следовать за навязанными идеологемами делает нас уязвимыми в отношении очередной агрессии. Эта уязвимость порождает самоуверенность у западных геополитиков, они ощущают эйфорию скорой и близкой победы, что делает их очень опасными. Нагнетаемая ими очередная волна русофобия вполне может захлестнуть мир и развязать новую, уже не гибридную войну.

Самуйлова И.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

РОЛЬ КАЧЕСТВА СООБЩЕНИЙ МАСС-МЕДИА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА

Сегодня от качества информации во многом зависит психическое и физическое здоровье человека. В связи с этим в современной науке обозначен широкий круг проблем от медико-психологических особенностей восприятия информации до понятия психологической травмы или формулирования критериев корректности информационного воздействия.

На кафедре политической психологии СПбГУ в последние годы активно ведутся теоретические и эмпирические исследования оценки качества социально-политических сообщений (объективность, полнота, понятность, непротиворечивость, практичность и др.), циркулирующих в СМИ, как с точки зрения анализа их психологического содержания, так и с точки зрения изучения представлений аудитории.

Обнаружены связи представлений аудитории СМИ о различных качествах социально-политических сообщений: 1) с психологическими защитами, которые актуализируются у человека в масс-коммуникационных ситуациях (избегание, управление, затаивание, блокировка); 2) с психическими состояниями (критичность, тревожность, напряженность, утомленность, любопытство, возмущение и др.); и 3) с другими критериями (потеря доверия к источнику информации, уменьшение способности конструктивного мышления и т.д.).

По результатам проведенных теоретических и эмпирических исследований, на факультете психологии СПбГУ разработана модель репрезентации российской политической коммуникации современными СМИ (2011), созданная на основе единства трех ключевых структурообразующих факторов: методологического, методического и практического. Данная модель включает в себя следующие переменные: 1) соблюдение психологических законов презентации социально-политической информации в СМИ; 2) соблюдение качества социально-политической информации, распространяемой в СМИ; 3) реализация социально-психологических функций политической коммуникации в СМИ; 4) психологические эффекты, производимые социально-политической информацией на индивидуальном и групповом уровнях; 5) психологические особенности аудитории СМИ; 6) степень соответствия социально-политической информации критериям информационно-психологической безопасности. Учет вышеуказанных переменных позволяет осуществлять более глубокий анализ масс-коммуникационных ситуаций и прогнозировать возможную психологическую реакцию аудитории на медиа-сообщения.

Свешникова Н.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПСИХОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ

Особое внимание ученых и мыслителей сегодня обращено к характеру трансформационных процессов человеческого сообщества в целом и отдельного индивидуума в частности, которые можно описать с позиций интенсивности, масштаба, скорости и глубины преобразований. Многие аспекты актуального состояния общества, как переходного, определяются противоречием между уровнем познания и практикой. Значительно возросла адаптивность человека к среде как биологического существа благодаря новым технологиям в медицине, энергетике и пр., что обеспечивает его все меньшую зависимость от среды обитания. При этом наблюдается все возрастающая агрессивность, архаизация моделей поведения, которая является следствием новых аспектов социального напряжения между технологически обеспеченными и технологически отсталыми, владеющими технологиями и пользующимися ими.

Человечество пришло к такой стадии развития, когда сила, количество и даже ум уже не являются преобладающими средствами борьбы. На смену оружию массового поражения пришли «знания массового поражения». Технологии пронизывают те только среду обитания человека и общности, но и проникают в сферу деятельности сознания. В качестве ведущих выступают информационные воздействия, как на индивидуальном уровне, так и на уровне массового сознания.

В последнее время возрастает внимание научного сообщества к исследованию феномена «информационная война», открывающее возможности осмысления ее психологических средств, механизмов и эффектов. В политической психологии информационное воздействие рассматривается на цивилизационном, социальном и индивидуальном уровнях. Информационное воздействие в современном обществе необходимо рассматривать не только с позиций актуального состояния общественной среды или обеспечения социального контроля, но учитывать потенциальное состояние социальной системы с позиций социального управления.

Особый акцент в психологических исследованиях информационного влияния приобретает осмысление общественной реальности как физической, когнитивной, нравственно-духовной. Внимание перемещается к исследованиям образной сферы, а именно представлений и их роли в смысловой регуляции поведения. Закономерности и особенности представлений могут раскрыть потенциал влияния информации на изменение сознания, так и устойчивости к ее воздействию. В наших исследованиях приоритетным является понимание механизмов влияния посредством символа и мифа. Важная роль символических структур и мифологизации жизненного пространства обнаруживается в процессах социального конструирования реальности и социального восприятия реальности. Такой подход позволяет рассматривать «информационную войну» как театр действий образов, создающих некую смысловую реальность. Важно отметить, что СМИ из активного деятеля на этом поле битвы превращаются в средство трансляции интерпретаций, а не фактов, которые перестают быть центральным звеном в информационном противостоянии.

Также следует отметить изменение роли и качества эксперта как актора информационного влияния: анализ, знание, независимость экспертного мнения подменяются констатацией или оценкой, мнением, отличающимся ангажированностью и зависящим от ситуации. Наблюдаются следующие особенности информационного воздействия: смена жанра - дискуссия заменяется на развлекательное ток-шоу, негативизация информации, большой удельный вес визуального и акустического рядов в сообщении, использование эмоционально-окрашенных именований, акцент на эффектах «хроникальности», использование социокультурных стереотипов и символов и пр.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

Большакова Л.В., Грачев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРОВЕРКА АДЕКВАТНОСТИ ПОСТРОЕННЫХ ЭКОНОМЕТРИЧЕСКИХ МОДЕЛЕЙ

Одной из основных задач эконометрического исследования является построение эконометрической модели, т. е. уравнения регрессии, которое в дальнейшем используется для анализа и прогноза возможных значений признаков (факторов), характеризующих тот или иной экономический процесс. После решения этой задачи, т.е. построения модели, возникает проблема оценки качества полученного регрессионного уравнения. Для того чтобы выяснить насколько хорошо полученная модель описывает реальную ситуацию, используют различные коэффициенты и статистические гипотезы, по значениям и результатам которых делают выводы об адекватности полученной модели.

Наиболее часто качество регрессионной модели оценивают по значениям коэффициента детерминации и средней ошибки аппроксимации, а также по результатам проверки статистических гипотез о значимости всего уравнения регрессии по критерию Фишера и значимости отдельных коэффициентов по критерию Стьюдента. Каждый из этих способов проверки адекватности обладает рядом недостатков, которые могут привести как к существенному занижению качества «хорошей» модели, так и к завышению качества «плохой» модели. Особенно это характерно для оценки качества модели по значению средней ошибки аппроксимации.

Средняя ошибка аппроксимации – это один из простых коэффициентов, который позволяет кратко охарактеризовать насколько соответствует смоделированный процесс реальному.

Под средней ошибкой аппроксимации понимают либо среднюю абсолютную ошибку аппроксимации, либо среднеквадратическую ошибку аппроксимации.

Очевидно, что значения этих ошибок для одной и той же задачи отличаются друг от друга. Принято считать, что если какая-либо из них не превосходит 12%, то регрессионная модель считается хорошего качества, т.е. адекватна действительности и по ней можно строить реальные прогнозы. Можно привести достаточно много примеров моделей хорошего качества, для которых значения средних ошибок аппроксимации не превосходят 12% и, наоборот, примеров моделей плохого качества с ошибками аппроксимации значительно более 12%.

Однако на практике существуют ситуации, в которых значения средних ошибок дают неверное представление о качестве и свойствах построенных моделей. Следовательно, выводы или прогнозы, сделанные по таким моделям, будут далеки от реальности.

Необходимо отметить, что неправильная оценка качества модели может быть получена не только по значению средней ошибки аппроксимации, но и по значению коэффициента детерминации, а также и при проверке значимости регрессионного уравнения по критерию Фишера. Однако одновременное проявление ошибочного оценивания качества регрессионной модели по всем перечисленным значениям коэффициентов и критериев маловероятно. Поэтому для получения более объективной оценки адекватности рассматриваемой регрессионной модели стоит рассчитать несколько коэффициентов и провести проверки соответствующих статистических гипотез.

Васькова А.В., Михайличенко Е.М.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации

МНОГОФАКТОРНАЯ МОДЕЛЬ ДЮПОН АНАЛИЗА ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ НА ПРИМЕРЕ ОАО «АВТОВАЗ» И ОАО «ГАЗ»

Модель Дюпона – метод финансового анализа через оценку ключевых факторов, определяющих рентабельность организации.

Целью финансового анализа является поиск путей максимизации прибыльности вложенного капитала для собственников и акционеров. В данной статье проведено исследование анализа эффективности деятельности двух ведущих компаний по производству автомобилей на российском рынке: АвтоВАЗ (автомобильный волжский автомобильный завод) и ГАЗ (Горьковский автомобильный завод).

Проанализирован организацию можно сказать, что показатель рентабельности продаж в 2014 году был очень низким, а в 2015 году снизился еще на 28,7 процентных пункта. Снижение прибыли на рубль реализованной продукции свидетельствует о снижении спроса на продукцию предприятия.

Оборачиваемость активов выросла на 0,14 оборотов. Это свидетельствует о незначительном улучшении использования активов.

Показатель рентабельности активов находился в отрицательном значении и составлял -15.1%, но на 2015 год произошел существенный спад на 39,3 %. Уменьшение уровня рентабельности активов может свидетельствовать о снижении уровня спроса на продукцию предприятия и о перенакоплении активов.

Финансовая зависимость также снизилась до -3,5 по сравнению с 2014 годом, в котором она составляла 4,7 пункта. Положительной считается тенденция к снижению коэффициента финансовой зависимости. Как и каждое предприятие, компания должна стремиться увеличивать долю собственных средств, с целью повышения стабильности функционирования.

Таким образом, показатель рентабельности собственного капитала тоже имел тенденцию к снижению, примерно на 119,1%.Это значит, что организация неэффективно использует капитал.

Далее предлагается сравнительный анализ за расчетный период 01.01.2015-01.06.2015 год и 01.01.2016-01.06.2016. Тенденция относительно рентабельности продаж и оборачиваемости активов остается прежней. Рентабельность активов также уменьшилась на 19, 2 %. Таким образом, подтверждается падение спроса на продукцию ОАО «АвтоВАЗ».

Финансовая зависимость увеличилась с -3.5 до -1.9 в 2016 году, но все равно составляет отрицательное значение. Это плохая тенденция по сравнению с 2014 и 2015 годом.

Рентабельность собственного капитала уменьшилась до -41,23%. Это примерно на 32,33 процентных пункта, что подтверждает неэффективность использования капитала в отчетном году.

АвтоВАЗ закончил первое полугодие 2016 года с чистым убытком в 27 млрд руб., следует из отчета компании по МСФО. Это в восемь раз больше показателя за аналогичный период прошлого года.

Основная причина такого большого убытка – обесценение внеоборотных активов, т.е компания очень мало использовала свои производственные мощности. АвтоВАЗ рассчитывает на поддержку со стороны акционера – Alliance Rostec Auto BV (СП «Ростеха», Renault и Nissan), владеющего пакетом акций в 74,51%. «Ростех» предлагает докапитализировать компанию и реструктурировать ее кредиты.

Среди факторов, оказывающих негативное влияние на рынок, можно выделить дальнейшее падение экономики России и покупательской активности населения, рост цен на автомобили на фоне ослабления российской валюты, а также высокую стоимость владения автомобилем.

ОАО «ГАЗ» является центром консолидации активов «Группы ГАЗ» – крупнейшего российского производителя коммерческого транспорта в РФ.

Анализ показывает, что в отчетном 2015 году показатель рентабельности продаж вырос на 0,1 процентный пункта. Это означает, что доля рынка, занимаемого продукцией ОАО «ГАЗ» увеличилась (рисунок 3).

Оборачиваемость активов снизилась на 0,34 оборота. Показатель свидетельствует о неэффективном использовании активов, что подтверждает снижение показателя рентабельности активов на 0,1%.

Финансовая зависимость увеличилась на 1, 5 пункта. Этот показатель также говорит о том, что необходимо больше собственных средств для покрытия заемных средств. Таким образом, рентабельность собственного капитала снизилась на 0,03%. В 2014 году она была 0,36%, а в 2015 году это значение составило 0,33%.

Далее предлагается сравнительный анализ за расчетный период 01.01.2015-01.06.2015 год и 01.01.2016-01.06.2016. Рентабельность продаж значительно увеличилась по сравнению с 2015 годом. На 01.06.2016 год показатель составил 3, 9%. Оборачиваемость активов также увеличилась на 0,03 оборота. Тем самым произошло увеличение рентабельность активов на 2,4%.Показатель финансовой зависимости остался на прежнем уровне.

Рентабельность собственного капитала увеличилась на 8,1%. ЗА 2 квартала 2016 года ОАО «ГАЗ» улучшило свое финансовое положения по всем показателям, используемых в анализе. Это говорит об успешной финансовой и маркетинговой политики компании.

В 2015 году происходило увеличение спроса на автомобили ГАЗ с дополнительными опциями:

- продажи автомобилей с ABS выросли на 56%;
- школьный автобус – рост продаж на 34%;
- промтоварные фургоны на базе среднетоннажных автомобилей – рост продаж на 20%.

Основные направления развития на 2016 г.:

- развитие экспортных продаж;
- стимулирование продаж, развитие сервисно-сбытовой сети;
- расширение продуктового предложения (в т.ч. на экспортных рынках);
- совершенствование системы отношений с поставщиками;
- улучшение качества гарантийного и пост гарантийного обслуживания.

Таким образом, автомобильный рынок, на примере двух ведущих компаний ОАО «АвтоВАЗ» и ОАО «ГАЗ», серьезно пострадал от кризиса, снижения покупательской способности у граждан и падения рубля на мировом рынке. Больше всего влияние этих факторов отразилось на финансовом положении компании АвтоВАЗ. Эффективная политика по сбыту и дифференциации продукта позволили ОАО «ГАЗ» получить прибыль в 2015 году.

Верзун Н.А., Касаткин В.В., Колбанёв М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский институт информатики и автоматизации РАН

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ И КИБЕРФИЗИКОБИОЛОГИЧЕСКИЕ ПРОИЗВОДСТВЕННЫЕ СИСТЕМЫ

Интернет вещей (Internet of Things, IoT) – одна из базовых технологий третьей платформы информатизации – сеть объектов двух типов: идентифицируемых «умных» вещей (УВ) – smart thing, без участия человека взаимодействующих между собой и с окружающей средой по стандартным протоколам, а также цифровых образов этих УВ, размещенных в вычислительных облаках. Внедрение IoT в промышленность обеспечивает переход к следующему поколению производственных систем (Индустрия 4.0) и привело к появлению термина «Индустриальный интернет вещей» (Промышленный интернет, Industrial Internet of Things, IIoT). IIoT – это разновидность интернета вещей, конвергенция производства и современных сетевых инфраструктур, которая коренным образом изменит традиционное промышленное производство.

Согласно концепции IIoT, к 2020-25 гг. промышленные роботы будут “понимать” происходящее вокруг, общаться друг с другом по протоколам интернета вещей, а на смену кибернетическим, физическим и биологическим системам придут киберфизикобиологические производственные системы, в которых физическая, биологическая и цифровая составляющие производственного процесса, будут образовывать единый комплекс, и совместно, в автоматическом режиме, реализовывать единый процесс.

Изменятся принципы функционирования производства: проектирование новых продуктов, организации маркетинга, логистики, использование различных ресурсов (сырья, материалов, оборудования и энергии) и пр. Все практические функции управления производством будут с возникновением киберфизикобиологических производственных систем переложены на вычислительную сеть. Наряду с механическими, автоматизации подвергнутся и управленческие операции, а за человеком останутся лишь действительно творческие задачи.

Рассматриваются технологии-компоненты IIoT, перспективы, основные направления и риски развития IIoT в России.

Верзун Н.А., Колбанёв М.О, Омельян А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СИСТЕМА РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ДЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РУСУРСАМ

Современные информационные технологии предполагают как можно более глубокую автоматизацию обработки информации, что подразумевает её перенос от главного обработчика – человеческого мозга к вычислительным средствам. Эти обработчики требуют совершенно различного представления информации: числовой код для автомата и символьно-графическое представление для человека. Пока существует человек, отказаться от представления информации на бумажном или каком-либо другом носителе в виде символьных, визуальных, графических образов невозможно.

Поэтому, результаты машинной обработки необходимо преобразовывать до вида, воспринимаемого человеком. Именно это преобразование зачастую «съедает» вычислительные ресурсы. Хотелось бы иметь структуру и носитель информации, объединяющий в себе символьно-графическое представления для человека и числовой код для автомата.

Как вариант решения этой задачи можно предложить объединение бумажного носителя с технологией радиочастотной идентификации, создающее структуру данных связывающую информацию на электронном и бумажном носителе. При этом необходимо предоставить человеку средства быстрого (параллельного) редактирования символьных данных и их структур в числовом виде. Бумажный документооборот сегодня не теряет своей актуальности, а применение систем радиочастотной идентификации позволяет соединить преимущества бумажного и электронного документооборота.

Рассматриваются особенности, возможности и ограничения применения систем радиочастотной идентификации в бумажном документообороте, при сопровождении архивных документов или документов длительного хранения, а также преимущества использования подобных систем по сравнению с другими средствами идентификации.

Володина А.А., Левкин И.М.
Россия, Санкт-Петербург, Университет ИТМО

МОДЕЛЬ ФОРМИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ ИНФОРМАЦИОННОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ

Формирование информационных угроз информационной структуры предприятия происходит на основании полученной, в ходе предпроектного обследования, информации, а также на основании произведенного анализа характеристик, рассматриваемого предприятия. Для построения модели необходимо выполнить ряд определенных задач. В первую очередь, необходимо выявить основные характеристики, рассматриваемого предприятия, среди которых:

- сведения об обрабатываемой на предприятии информации, включая состав защищаемых информационных ресурсов, содержащих информацию ограниченного доступа;
- законодательные и нормативные правовые акты в сфере информационной безопасности, регулирующие деятельность предприятия;
- сведения об используемых предприятием информационных системах, включая сведения о собственниках и владельцах, заказчиках их создания и разработчиках данных информационных систем;
- описание технологического процесса обработки информации;
- описание процесса передачи информации между участниками технологического процесса обработки информации.

Следующей задачей является определение возможных каналов утечки информации, обрабатываемой в информационных системах предприятия, а также определение перечня мероприятий по их устранению и ограничению. Как правило, возможные каналы утечки информации подразделяются на классы. Обычно это прямые и косвенные каналы утечки информации. Под прямыми каналами понимается инсайдерская деятельность, а также прямое копирование информации. В роли инсайдера может выступать обслуживающий персонал предприятия, имеющий доступ к информации ограниченного доступа, обрабатываемой на предприятии. К косвенным каналам относится кража носителей информации, также их утеря, перехват информации, прослушивание и т.д. На предприятии к этому классу могут относиться основные и вспомогательные технические средства и системы предприятия, в том числе и каналы передачи данных ЛВС.

Следующим этапом является рассмотрение информационной структуры предприятия. Определяются взаимосвязи, составляется карта информационных потоков предприятия.

После произведенного анализа характеристик предприятия, а также возможных каналов утечки, необходимо выявить всевозможные угрозы безопасности информации, обрабатываемой на предприятии, а также в его информационных системах. Для этого определяются источники угроз безопасности информации, актуальные для рассматриваемого предприятия, приводится перечень всех возможных угроз, а затем составляется методика определения возможных угроз безопасности информации, обрабатываемой на предприятии.

По итогам произведенного анализа возможных угроз безопасности формируется перечень актуальных угроз, представляющие наибольшую опасность для информации, обрабатываемой на предприятии и в его информационных системах.

Таким образом, модель формирования информационных угроз информационной структуры предприятия будет состоять из следующих этапов:

1. Сбор информации о предприятии
2. Определение информационной структуры предприятия
3. Анализ существующих информационных угроз
4. Формирование перечня информационных угроз с наибольшей вероятностью их реализации на рассматриваемом предприятии.

Головкин Ю.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ СЛОЖНЫМИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ В НЕШТАТНЫХ СИТУАЦИЯХ

В процессе эксплуатации сложных технических систем (СТС) в результате отказов техники, ошибок операторов и воздействия внешней среды могут возникать нештатные ситуации (НС). Проблема обеспечения безопасности функционирования является комплексной задачей, одной из важных направлений решения которой – разработка моделей и программных средств, повышающих качество формирования управляющих воздействий для обеспечения эффективного автоматизированного управления сложными техническими системами в нештатных ситуациях.

Как показывает опыт, обеспечить требуемый уровень безопасности функционирования с использованием только автоматического режима не удается. Особенностью многих НС является многоэтапный характер их развития, при котором каждый этап характеризуется своеобразным поведением объекта управления и необходимыми управляющими воздействиями для ликвидации

опасных последствий. Как правило, алгоритмы управления ориентированы на обнаружения НС и ее ликвидации в начальной стадии возникновения, но не контролируют развитие ситуации вглубь. Следует отметить, что при возникновении НС значительно возрастает роль оператора в процессе управления. В этих условиях возникают задачи повышения уровня автоматизации процесса управления при возникновении НС и организации оптимального взаимодействия автоматики и оператора в интересах обеспечения надежного и безопасного функционирования.

Процесс управления в нештатных ситуациях характеризуется большой психологической нагрузкой оператора и малым резервом времени. Это повышает вероятность ошибочных действий оператора. Успешность деятельности оператора в НС в значительной степени зависит от той информации, которой он располагает. Непосредственными причинами ошибок оператора могут также быть: неполная, ложная и неопределенная информация о ходе протекания НС. При управлении в НС оператор должен быть максимально освобожден от процесса поиска и переработки большого объема информации. Поэтому в процессе управления оператора необходимо информировать не только о возникновении НС, но и выдавать ему сообщения (рекомендации) о действиях по управлению в этих ситуациях.

Таким образом, для повышения эффективности управления СТС при возникновении НС, необходимо:

- своевременно и точно обнаруживать возникновение НС;
- контролировать развитие НС;
- информировать оператора о ходе протекания НС и необходимых действиях по управлению.

Модель процесса управления предлагается задавать в виде ориентированного графа. Вершины графа соответствуют ситуациям процесса управления, а дуги задают возможные переходы ситуаций. Дугам ставятся в соответствие предикаты, контролирующие условия перехода ситуаций. Выявлено, что для адекватного описания процесса управления ситуационная модель может иметь многоуровневую структуру, при которой любой вершине (ситуации) ставится в соответствие некоторая внутренняя модель.

Рассматриваются вопросы разработки программного обеспечения для моделирования процессов управления в нештатных ситуациях в интегрированной среде программирования. Процесс визуального программирования включает в себя два этапа: создание пользовательского интерфейса и написание программного кода, который придает элементам интерфейса определенную функциональность. Пользовательский интерфейс создается с использованием визуальных компонентов на экранных формах, каждый из которых характеризуется своими свойствами и методами.

Программное обеспечение имеет многоуровневую модульную структуру. Модули верхнего уровня выполняют более общие функции и вызывают модули нижних уровней, в которых детализируется решение задачи. Программа контролирует текущее состояние процесса управления по ситуационной модели и запускает соответствующие процедуры, которые задают необходимые управляющие действия.

В заключение можно отметить, что использование ситуационных моделей приводит к повышению качества формирования управляющих действий и увеличивает эффективность автоматизированного управления сложными техническими системами в нештатных ситуациях.

Елизаров М.А. Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МОДЕЛЬ ИДЕНТИФИКАЦИИ МЕТОК В RFID-СИСТЕМЕ

Организация учета, контроля и управления, основанная на электронной идентификации находит все большее применение в различных сферах человеческой деятельности. Объектом идентификации при этом может быть человек, животное, транспортное средство, контейнер с грузом, изделие в процессе производства и много другое. Среди способов, реализующих этот процесс, распространение получила радиочастотная идентификация (RFID) благодаря своей высокой степени защиты от взлома.

Радиочастотная идентификация (RFID, Radio Frequency IDentification) – метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся на специальных носителях, называемых RFID-метки, или просто метки.

Общая схема RFID-системы состоит из трех базовых компонент:

- считывающего устройства (передатчик/приемник, или просто считыватель);
- антенны;
- RFID-меток (транспондеров) со встроенной антенной, приемником и передатчиком.

Считывающее устройство активирует метку, после чего происходит передача с нее информации на считывающее устройство. Считыватель может иметь различное исполнение – от простого переносного сканера до стационарного устройства.

Антенна излучает электромагнитные волны, активизирующие RFID-метку, что и позволяет производить запись и считывание данных с этой метки. Антенна является своеобразным каналом между меткой и считывателем. Она встраивается, например, в специальные сканеры, ворота, турникеты, дверные проемы и т.п. для получения информации от предметов или людей, перемещающихся через зону действия антенны. Антенны также различаются по размерам и форме. Конструктивно антенна и приемопередатчик могут находиться в одном корпусе. Сигнал, поступающий с антенны, демодулируется, расшифровывается и передается через стандартный интерфейс в компьютер для дальнейшей обработки.

Физической базой RFID-метки является микрочип, испускающий радиочастотные волны, попадающие на считывающее устройство, поэтому без знания сложных кодов и отсутствия специального оборудования взломать RFID-метку проблематично. Внешне она представляет собой тонкую этикетку. Метка может содержать данные о типе объекта, стоимости, весе, температуре, данные логистики и вообще любой информации, которая может храниться в цифровой форме. Подделать метку практически невозможно.

Функционирование RFID-системы, состоящей из считывателя и группы меток, входящих в зону опроса считывателя происходит в режиме мультидоступа. В таком случае необходимо учитывать возможность одновременной передачи данных сразу от нескольких меток, что приводит к одновременному появлению модулированных сигналов на входе считывателя и как следствие их взаимному искажению. Данное явление называется коллизией, возникновение которой не позволяет получить достоверную информацию. Более того, с ростом количества меток в поле считывателя вероятность появления коллизии возрастает. Для борьбы с коллизиями управляющая программа RFID-системы должна включать антиколлизионную процедуру, распознающую и устраняющую такие ситуации.

Статья посвящена моделированию антиколлизионной процедуры идентификации меток, реализованной во временной области. Средствами имитационного моделирования (ИМ) оценивается время, необходимое для идентификации меток, находящихся в поле считывателя.

ИМ инвариантна для количества меток, находящихся в зоне действия считывателя, значений продолжительности считывания одной метки и значений диапазона генератора случайных задержек активации меток.

Емельянов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПРИМЕНЕНИЕ СЕТЕВЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ ПРЕДПРИЯТИЙ МАЛОГО БИЗНЕСА

В настоящее время применение сетевой инфраструктуры на предприятиях является основой функционирования вне зависимости от сферы деятельности конкретной организации. Большинство ежедневных задач выполняется при помощи различных ИТ, реализованных в программных продуктах. При этом используется как локальное ПО (текстовые процессоры, электронные таблицы и т.д.), так и сетевое, базирующееся на схемах совместного использования и обеспечении множественного доступа с клиент-серверной архитектурой (распределённые информационные системы, облачные сервисы). Для обеспечения функционирования программно-аппаратного комплекса и сетевых подсистем необходимы существенные инвестиции: на этапах закупки оборудования и ПО, проектирования внутренней сети предприятия, поддержке и модернизации рабочих мест пользователей. Кроме того, каждое рабочее место сотрудника требует дополнительных капиталовложений, и, чем больше штат – тем большую арендную плату нужно вносить.

Альтернативой классической форме работы является схема удалённого сотрудничества. Реализация схемы базируется на повсеместном распространении сети Интернет с широкополосным доступом - как в проводных, так и в беспроводных вариантах, улучшению ценовой политики для конечных пользователей, активном использовании безлимитных тарифов. С помощью средств удалённого подключения (VPN-туннелирование) можно создавать криптографически защищённые каналы связи через сеть Интернет между серверами организации и сотрудниками предприятия, выполняющими повседневные задачи компании на своих домашних компьютерах. Подключаясь к VPN-серверу, пользователь получает доступ к информационным ресурсам организации, что позволяет ему работать точно так же, как если он присутствует физически на рабочем месте в организации.

Программно данная схема может быть реализована на базе операционных систем Windows либо Linux. Использование программного обеспечения прокси-сервера в связке с VPN-сервером позволит выполнять безопасные удалённые подключения с надёжной системой аутентификации, осуществлять контроль за передаваемыми данными, внедрять эффективные политики безопасности, связывать территориально разнесённые офисы предприятия в единую сеть.

При использовании схемы удалённого сотрудничества будет выигрывать как работодатель (снижение затрат на аренду помещений, аппаратно-программный комплекс, сетевую

инфраструктуру), так и сотрудник (отсутствие необходимости ежедневно тратить время и деньги на перемещения от дома до предприятия; возможность выполнять работу в более комфортных условиях из любой точки планеты).

Касаткин В.В., Колбанёв М.О., Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный экономический университет

АНАЛИЗ ПРОЦЕССОВ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ ДАННЫХ

Объем цифровой вселенной вырос настолько, что измеряется в зета- и йотабайтах, при этом размеры массивов хранения могут достигать не только тера-, но и петабайт. Стоимость сохранения 40 зетабайт данных, а именно такого объема по прогнозам достигнет цифровая вселенная к 2020 г., при ценах, установленных в облачных хранилищах Mail.ru online, равна ~0,5 трлн. руб/мес, а в облачном хранилище Google Cloud Storage Nearline – не менее ~$20 млрд. в мес. Необходимо учитывать, что требуемое время сохранения некоторых видов данных может измеряться не только десятками лет, как, например, при архивном хранении, но и сотнями и даже тысячами лет, если речь идет о фамильных данных, или данных, влияющих на выживание будущих поколений человечества.

В докладе рассматриваются достоинства и недостатки хранения данных на личных запоминающих устройствах и в публичных и частных облаках.

Показано также, что решение задачи долговременного сохранения данных требует разработки новых технологий, учитывающих энергетические характеристики информационных систем. Широко распространенные сегодня технологии сохранения данных не ориентированы на долговременное сохранение, они предназначены для использования в системах реального времени, позволяют многократно изменять относительно небольшие объемы данных, обеспечивать их доставку пользователям по инфокоммуникационным сетям. Конкурентоспособность таких систем тем выше, чем выше плотность записи на информационный носитель и меньше время записи/считывания данных. Еще одной целью разработчиков является уменьшение времени доступа к данным. Все типы носителей для таких систем можно проектировать, исходя из времени гарантированного сохранения, ограниченного годами. Этого достаточно, чтобы удовлетворительно работать в любых системах реального времени, но не соответствует задачам долговременного сохранения.

Килин В.С.
Россия, Санкт-Петербург, Университет ИТМО

РЫНОК ИТ-АУТСОРСИНГА В СТРУКТУРЕ ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

Мировой рынок ИТ-аутсорсинга, несмотря на непростую экономическую ситуацию, продолжает расти за счет активного развития технологий и растущих ожиданий покупателей.

По данным исследовательской компании Gartner, расходы на ИТ-аутсорсинг будут увеличиваться вплоть до 2018 года, а подъем в 2015 году будет замедлен, но все-таки составит в среднем 4,5 %.

При этом акцент расходов будет сдвигаться от традиционных, на мировых рынках, услуг ИТ-аутсорсинга, таких как поддержка ЦОДов и корпоративных информационных систем, на новые — стандартизированные и отраслевые предложения, в том числе облачные сервисы.

Что касается российских показателей, то они следуют мировым тенденциям. По итогам 4 квартала 2014 года рост рынка ИТ-аутсорсинга в нашей стране составил 4 % (по данным IDC). И хотя в России движение потребителей в сторону ИТ-аутсорсинга начало появляться лишь недавно, заказчики продолжат проявлять активный интерес к данной сфере услуг, особенно большой рост покажет спрос на аутсорсинг ИТ-инфраструктуры. Начав с простых технических функций, клиенты рынка становятся все более опытными, они постепенно, но уверенно двигаются к более сложным и комплексным задачам. А соглашение об уровне предоставления услуг (SLA), удовлетворяющее требованиям бизнеса, становится ключевым показателем при принятии решения о заключении контракта.

Развитие ИТ-аутсорсинга и индустрии услуг внутри страны также не удовлетворяет возлагаемым требованиям и достаточно отстает от необходимого уровня. Причин такого отставания множество, однако, можно выделить среди наиболее важного низкого уровня развития малого и среднего бизнеса, конкуренции, а также достаточно слабая интеграция с мировой экономикой.

Причины перехода на ИТ-аутсорсинг имеют свою отраслевую специфику. Для государственных учреждений к их числу относятся – жестко ограниченный ИТ-бюджет, получение доступа к новым технологиям и профессиональным ресурсам, необходимость роста объемов и улучшение качества IT-услуг без увеличения численности персонала; для финансовых организаций – сокращение операционных расходов, в промышленности – повышение эффективности производства, в оптовой и розничной торговле – обеспечение непрерывности бизнеса.

ИТ-аутсорсинг неизбежно возникает как гибкая форма организации сетевых связей. Если сетевой доступ к экономическим объектам и агентам обеспечен, то проблема установления и поддержания нужных связей между ними в сетевой экономике превращается в проблему организации эффективного процесса непрерывных контактов и обмена информацией, что дает большой потенциал развитию ИТ-аутсорсинга. Сегодня место ИТ-аутсорсинга, в структуре экономической системы довольно неоднозначно и определить его достаточно сложно. Для того чтобы рассмотреть рынок ИТ-аутсорсинга, как систему экономических отношений, удобно, как нам кажется, использовать кластерную форму организации экономики.

Теория В. Фельдмана базируется на том, что механизмы, которые ведут к образованию кластеров основаны на диверсификации, которая, в свою очередь, следует модели «затраты-выпуск». Компании выигрывают, имея возможность делиться положительным опытом и снижать затраты, совместно используя одни и те же услуги и поставщиков. Постоянное взаимодействие способствует формальному и неформальному обмену знаниями, сотрудничеству между организациями с взаимодополняющими активами и профессиональными навыками.

Аутсорсинг позволяет компании-клиенту снизить расходы на ИТ поддержку, оптимизировать работу своей информационной структуры и полностью сосредоточиться на развитии своего основного бизнеса. Все это позволяет говорить о важности аутсорсинга в ИТ сфере для отечественной экономики.

В результате, можно считать, что у рынка ИТ-аутсорсинга есть своя особенная черта. Она заключается в том, что потенциальными потребителями этого рынка, в отличие от остальных, являются все кластеры экономики: поставщики, инжиниринговые фирмы, производители, кредитные организации, профессиональные объединения, органы власти и общественные организации и т.д. На сегодняшний день развитие рынка ИТ-аутсорсинга в России только точечное, поэтому данную трактовку можно использовать скорее с общей – теоретической точки зрения, хотя в некоторых странах ИТ-аутсорсинг востребован почти во всех отраслях экономики.

Коломойцев В.С.
Россия, Санкт-Петербург, Университет ИТМО

О ПРОБЛЕМЕ ПРОЕКТИРОВАНИЯ БЕЗОПАСНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Современные экономические системы, обрабатывающие множество данных, часто подвергаются кибернетическим атакам как извне, так и изнутри. В основном, размер организации, использующей вычислительные системы для решения необходимых для нее задач, практически не влияет на виды и методы атак на данные системы. Число вычислительных систем в организации и их размер имеет прямое влияние на количество атак в единицу времени (т.к. из-за увеличения размера вычислительной системы, растет и количество важных для злоумышленников данных) и на то, какой вид атак станет наиболее вероятным.

Вопрос организации защиты вычислительной системой, хранящей и обрабатывающей информацию, является одним из ключевых в области информационной безопасности. Какие методы и средства информационной защищенности применить в вычислительной системе, целесообразность использования одной и более независимых вычислительных систем для решения поставленных перед задач; как организовать подключение вычислительной системы к внешним сетям и к другим вычислительным системам организации. Все эти и многие другие вопросы встают перед руководством организации и проектировщиком системы безопасности при создании высоконадежной, быстродействующей и безопасной вычислительной системы.

При проектировании вычислительной системы необходимо точно определиться с тем, какие данные и в каком количестве будут обрабатываться и храниться в вычислительной системе. Если данные имеют однотипный характер и частота доступа к ним извне сравнительно редка, то, возможно, при выборе средств и мер обеспечения защиты этих данных стоит сделать упор на использование криптографических и антивирусных средств (включающих в себя программный межсетевой экран). Если необходимо часто передавать данные другим вычислительным системам корпоративной или внешней (неподконтрольную самой организации) сети, то дополнительно применяются аппаратные средства межсетевого экранирования для контроля за доступам к ресурсам вычислительной системы.

Не менее важным является также и то, как много групп сотрудников будет работать с данными вычислительной системы. От того, сколько одновременных запросов от разных групп пользователей к данным будет происходить, и будет ли работа с данными вестись удаленно (путем подключения к единому серверу или же нет), зависит и то, как лучше будет произвести резервирование критически важных узлов вычислительной системы и каналов связи между ними. Это является необходимым для снижения нагрузки на каждый из узлов и каналов связи по отдельности и, тем самым, повышает надежность и быстродействие всей системы в целом. Так, например, если в вычислительной системе есть дата-центр, на котором хранится вся необходимая для ежедневной работы информация, то ни при каких обстоятельствах нельзя допустить, чтобы к нему вел один-единственный канал передачи

информации. В таком случае, любая внештатная ситуация (не только по вине злоумышленника), приводящая к выведению из строя данного канала передачи информации (или же самого дата-центра), несет огромные финансовые потери для организации как из-за времени простоя работы организации, так и из-за возможного уничтожения (потери) данных организации.

Стоит также отметить, что, когда у отдельного вычислительного узла больше одного пользователя, то обязательным для достижения высокого уровня безопасности вычислительной системы, в которую он включен, является использование средств разграничения доступа. Эти средства могут быть внедрены как в виде программной, так и в виде аппаратной реализации. Средства разграничения доступа направлены на создание таких условий работы с вычислительным узлом, при которых любой посторонний пользователь узла (как внешний, так и внутренний нарушитель) не сможет получить доступ к хранящимся или обрабатываемым на узле данным, а также настроить работу узла под свои нужды (например, для ретранслирования зловредных данных на другие узлы вычислительной системы).

Таким образом, вопрос проектирования вычислительной системы и применение в ней тех или иных средств и мер обеспечения информационной безопасности требует комплексного и серьезного подхода. Необходимо учесть множество факторов и условий, в том числе не только технического, но и организационного характера.

Кузьмина Е.И.
Россия, Санкт-Петербург, Санкт- Петербургский государственный экономический университет

ФЕНОМЕН ЭФФЕКТИВНОСТИ КОМПАНИИ ALIBABA GROUP ДЖЕКА МА

Выполнен анализ особенностей компании ALIBABA GROUP в конкурентной среде электронной коммерции. Установлены факторы эффективности бизнеса компании. Среди факторов успеха решающим стал талант и исключительные способности его основоположника и руководителя Джека Ма. Особую роль играет стратегия, которую определяет Ма для развития компании. Стратегические цели и методы их достижения учитывают отличия восточного рынка от западных. Установлено, что принципы управления бизнесом Джека Ма имеют важное значение для последователей – представителей виртуального бизнеса.

Левкин И.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ ПРОДУКТОВ (УСЛУГ)

Экономическая значимость информационных продуктов (услуг) на рынке определяется их потребительскими свойствами, то есть способностью удовлетворять конкретные запросы пользователей. К основным потребительским свойствам можно отнести:

- релевантность – способность информации соответствовать конкретным запросам потребителя;
- полнота – способность исчерпывающе характеризовать отображаемый объект;
- своевременность – способность соответствовать нуждам потребителя в нужный момент времени;
- достоверность – свойство информации не иметь явных и скрытых ошибок;
- доступность – возможность получения информации конкретным пользователем; защищенность – недопустимость несанкционированного использования или изменения;
- эргономичность – удобство формы или объема информации с точки зрения конкретного пользователя; независимость качества (ценности, полезности) информации от ее количества и затрат на поиск, обработку, предоставление;
- адресность информации (ориентация на конкретные категории пользователей и целевые установки);
- временные затраты на подготовку и использование информационного сообщения; оперативность предоставления информации, сроки удовлетворения запроса; пригодность к многоаспектному поиска информации;
- надежность представленных данных (сроки их актуализации, достоверность источников информации); аспектность охвата темы, проблемы в пределах основной и смежных областей знания и практической деятельности; возможность машинной обработки и распространения информации;
- комфортность предоставления и использования (оптимальный объем информации, четкий шрифт, качественное изображение, дружественный интерфейс, детальность пользовательских инструкций);
- доступность (по каналам связи, видам носителей, цене);
- защищенность от несанкционированного доступа и воздействия; условия хранения и актуализации (для информационных продуктов); эстетичность, современный дизайн, фирменный стиль и др.

Левкин И.М.
Россия, Санкт-Петербург, Университет ИТМО

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ ФОРМИРОВАНИЙ МЧС В РАЙОНАХ КРУПНОМАСШТАБНЫХ КАТАСТРОФ

К важнейшим особенностям крупномасштабных катастроф, с точки зрения условий ликвидации их последствий, можно отнести следующие:

- значительный пространственно-временной размах;
- высокая динамика изменения обстановки в районе катастрофы;
- существенные ограничения доступа личного состава подразделений МЧС в отдельные район катастрофы.

Перечисленные и иные особенности затрудняют действия подразделений МЧС, участвующих в ликвидации последствий крупномасштабных катастроф. В первую очередь это связано с отсутствием эффективной системы их информационного обеспечения.

Основным средством получения полной информации о районе бедствий являются космические информационные системы. Они обладают экстерриториальностью, всепогодностью (радиолокационные системы наблюдения), высокими производительностью и информативностью (получение качественных мультиспектральных изображений в видимом, инфракрасном, и сантиметровом диапазонах электромагнитного спектра). Однако основным недостатком этих систем является их низкая оперативность, связанная со значительными затратами времени:

- во-первых, на прохождение управляющей информации по контуру: формирование заявки на съемку района катастрофы – планирование работы бортовой специальной аппаратуры – закладка программы работы на борт космического аппарата – выход космического аппарата в район съемки земной поверхности (район катастрофы) – доставка полученной информации в наземные органы обработки;
- во-вторых, на обработку (дешифрирование) больших объемов видовой информации.

Основными направлениями повышения эффективности информационного обеспечения действий формирований МЧС являются следующие.

1. Включение в информационно-аналитические региональные структуры МЧС РФ информационных подразделений, интегрированных в информационно-управляющий контур Единой территориально-распределенной информационной системы дистанционного зондирования Земли (ЕТРИС ДЗЗ). На эти группы должны быть возложены такие обязательные задачи, как:

- поддержание постоянной связи с органами системы запуска и управления космическими аппаратами;
- плановое получение из ЕТРИС ДЗЗ космической информации о зоне региональной ответственности, ее дешифрирование с целью мониторинга текущей обстановки на земной поверхности и передача обработанной информации в базу мобильного наземного комплекса приема обработки и распределения;
- разработка текущих планов применения космических аппаратов для мониторинга земной поверхности в зоне региональной ответственности и оперативных планов высоко периодичной съемки районов катастроф (в рамках выделенного планового или наращенного ресурса космических информационных систем).

2. Создание на базе контура космической информации интегрированной информационной системы, обеспечивающей:

- сбор, комплексную обработку и визуализацию информации от различных информационных средств космического (из ЕТРИС ДЗЗ), воздушного и наземного базирования;
- непосредственный прием информации от космических систем ДЗЗ;
- автоматическое доведение обработанной информации на индивидуальные средства ее отображения в требуемом объеме.

3. Разработка адаптивных алгоритмов комплексной обработки информации различных видов, реализующих следующие основные принципы:

- принцип автоматической привязки получаемой информации от различных средств мониторинга к геоинформационной подложке;
- принцип адаптивного оптимального распределения средств обработки по видам поступающей информации;
- принцип последовательного (последовательно-параллельного) применения методов обзорной и детальной обработки информации;
- принцип согласованного применения режимов дежурной, плановой и оперативно-целевой обработки информации.

Левкина С.В.
Россия, Санкт-Петербург, ООО «Витамед»

ЧИСЛЕННАЯ ОЦЕНКА ЦЕННОСТИ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

Одним из важнейших свойств информации является ее ценность. Наиболее распространенной оценкой ценности информации является мера А.А. Харкевича и М.М. Бонгарда: связанная с вероятностью достижения цели до получения информации и после ее получения.

Анализ информационных источников, используемых для информационного обеспечения деятельности объектов свидетельствует о том, что в каждом из них содержатся фрагменты информации (описания информационных признаков), которые могут быть использованы для решения различных информационных задач, стоящих на задании соответствующей информационно-аналитической структуры. Таким образом, ценность информационного источника должна оцениваться по степени решения при его помощи совокупности информационных задач с учетом важности каждой из них.

Данный подход может быть использован и в других методиках оценки ценности информационных источников, предложенных В.И. Корогодиным, М.В. Волькенштейном и другими.

Наличие численной оценки ценности информационных источников в процессе информационного обеспечения деятельности различных объектов позволяет определить:

- приоритеты в их поиске и добывании;
- последовательность их обработки при решении совокупности информационных задач;
- меры по их защищенности (при наличии оценки нанесения вреда при утечке информации из информационного источника) и т.п.

Минаков В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УМНЫХ ИННОВАЦИЯХ: ПРИЗНАКИ, СВОЙСТВА

Ряд современных инновационных продуктов (в их числе товары, услуги, способы управления и др.), являясь результатами интеллектуального труда человеческого капитала, одновременно проявляют интеллектуальные свойства в процессе их использования. Например, беспилотные аппараты обладают способностью ориентации на местности в режиме реального времени. А в зависимости от рельефа вырабатывают команды управления двигателем, изменения направления полета, и ряд других. Основой такого инновационного решения являются информационные технологии. В бытовых роботах-пылесосах функциональные задачи решаются на основе знаний, производимыми их информационными ресурсами.

Актуальной становится задача изучения особенностей, свойств и признаков инновационных информационно-технологических решений, обладающих искусственным интеллектом, свойством формирования знаний, которые можно определить как умные инновации.

Дефиницию «умные инновации» можно представить следующим образом. «Умные инновации» (или «смарт инновации») – это новшества (нововведения), обладающие такой совокупностью отличительных признаков, которые обеспечивают потребительскую ценность и положительный эффект от использования производимых знаний.

Можно выделить следующие признаки смарт инноваций:

- производство знаний информационными технологиями искусственного интеллекта в режиме реального времени при эксплуатации инновационного продукта;
- работа в автономном автоматическом режиме;
- способность адаптации при изменении экзогенных и эндогенных условий работа;
- превосходство над аналогами за счет смарт свойств;
- знания являются решающим фактором распространения инновационных продуктов на всех этапах жизненного цикла
- возможность замещения путем загрузки в цифровые гаджеты умных устройств новых версий программного обеспечения;
- работа в компьютерных сетях (Интернет или локальных в зависимости от потребности);
- использование операционных систем и программных средств реализации «умных функций».

Приведенные отличительные признаки позволяют выделить отдельный класс инноваций: смарт инновации. К такому классу можно отнести парк широко используемых смартфонов, смарт телевизоров, ряд персональных и планшетных компьютеров, ноутбуков, умных часов и браслетов, устройств хранения информации, выполняющих ее запись как по голосовым командам человека, так и по заданным алгоритмам, критериям, предпочтениям пользователей. Налажено производство умных роутеров, видеокамер, плееров, устройств шумоподавления и других. Смарт системы время разрабатываются для автомобилей (зарядные устройства и замки, системы контроля и управления автомобилем). Выделенный класс инноваций включает и программные средства с компонентами искусственного интеллекта решения таких функциональных задач, как игра в шахматы, задач

распознавания образов, классификации, кластеризации, перевода текстов, голосового управления гаджетами и других.

Следует указать, что ряд умных инновационных устройств может быть агрегирована в систему, обеспечивая им в сравнении с аналогами эмерджентность, то есть новые свойства, не присущие ни одному из компонентов, образующих такие системы. Например, системы «умных домов» обладают бесспорными преимуществами по отношению к автоматизированным решениям каждой единицы оборудования дома. Кроме того, системное умное решение минимизирует энергопотребление при обеспечении одного и того же уровня комфорта. Обобщая, можно резюмировать, что пользователь умного дома задает только цель и задачи, в то время как способ их достижения вырабатывается и реализуется компьютерной интеллектуальной системой. Заметим, в умном доме задача достижения цели решается системно, причем с взаимодействием компонентов, которые в этом случае образуют мультиагентную систему. Концепция и системные решения «умный город» развивают такой подход. Ключевые информационно-технологические решения такого города к настоящему времени созданы и проверены на практике.

Аналогичная ситуация сложилась и в разработках умного транспорта, безопасность и комфортность которого трудно переоценить.

Экономически эффективным инновационным решением являются умные производственные подразделения и даже умные предприятия. Поддержка принятия решений в системе управления их ресурсами и даже решения вырабатываются умными системам автоматизации, которым в качестве цели задаются показатели эффективности.

Изложенная трактовка умных инноваций на базе информационных систем и технологий открывает принципиально новую возможность замещения инноваций путем совершенствования версий программного обеспечения при неизменности аппаратных средств.

Михайлова А.С.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

СИСТЕМА МОТИВАЦИИ ПЕРСОНАЛА НА ПРЕДПРИЯТИИ

Одним из факторов, влияющих на повышение результативности хозяйственной деятельности современных предприятий, а также повышения их конкурентоспособности на рынке является эффективное управление трудовыми ресурсами, где особое место занимает мотивация работников. Умение руководителей вовремя замечать и определять факторы, которые влияют на трудовую активность работников, в настоящее время является достаточно ценным рычагом управления, поскольку активизирует скрытые резервы повышения производительности труда.

Важную роль в построении объективной и эффективной системы мотивации играет Ключевой индикатор выполнения (KPI) или Ключевой показатель эффективности (КПЭ).

KPI представляет собой систему, используемую для достижения главных целей любого бизнеса, таких как привлечение и удержание потребителей (клиентов), рост профессионализма сотрудников, увеличение доходов и снижение затрат. Пять аргументов в пользу применения системы KPI в мотивации персонала:

1. 100%-ная ориентация на результат – сотрудник получает вознаграждение за достижение результата и за выполнение работ, которые должны привести к результату;
2. управляемость – позволяет корректировать направленные усилия сотрудников без серьезной модификации самой системы при изменении ситуации на рынке;
3. справедливость – достойная оценка вклада сотрудника в общий успех компании и справедливое распределение рисков (между сотрудником и компанией) в случае неуспеха;
4. понятность – сотрудник понимает, за что компания готова его вознаграждать; компания понимает, за какие результаты и сколько она готова заплатить;
5. неизменность – любой сотрудник выстраивает свою работу в соответствии с системой мотивации. Если в определенный момент система меняется, то часть усилий сотрудника уходит впустую. Компания определяет «правила игры» для сотрудников, и если вдруг решит спонтанно их поменять, то лишится доверия «игроков».

Михайличенко Е.М., Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена, Финансовый университет при Правительстве Российской Федерации, Санкт-Петербургский государственный институт психологии и социальной работы

ТЕХНОЛОГИИ «ИНТЕРНЕТ - МАРКЕТИНГА» КАК СРЕДСТВО ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ

В условиях глобализации экономики деятельность многих индивидуальных предпринимателей (ИП) зависит от тенденций развития глобальных торговых сетей, которые устанавливают на рынке цены, обеспечивают широкий ассортимент и высокое качество продукции, что приводит к повышению

конкуренции и требует от каждого ИП принятия значительных усилий и мер по повышению своей конкурентоспособности. В российской экономике для повышения конкурентоспособности ИП обычно используются следующие методы: 1) установление более низких цен на продукцию, чем цены у конкурентов; 2) расширение ассортимента; 3) расширение торговых площадей; 4) улучшение обслуживания клиентов; 5) усиление и улучшение рекламы, продвижение продуктов; 6) улучшение и расширение систем распределения продуктов; 7) стимулирование сбыта. В статье предлагается использовать ряд инновационных методов повышения конкурентоспособности ИП на основе WEB – технологий, в области организации и обучению ИП розничной торговли товарами спортивного питания. Для этого ИП должен разработать стратегию, план работ и график повышения своей конкурентоспособности, с учетом краткосрочных, среднесрочных, долгосрочных мероприятий. По мнению авторов, структура online-маркетинга включает в себя следующие процессы: интернет-интеграция, информационный менеджмент, PR, службу работы с покупателями, продажи.

Для использования технологии «Интернет - маркетинга» с целью повышения конкурентоспособности ИП требуется организовать: 1) поиск денежных средств: а) инвестирование свободных денежных средств в инфраструктуру сайта или получение кредитов в банке; б) аренду интернет ресурсов для продвижения товаров; в) поиск спонсоров; г) привлечение соинвесторов; 2) кадровое обеспечение: а) повышение квалификации работников; б) набор сотрудников специализирующихся в сфере IT; в) обмен опытом; г) регулярное планирование и контроль работы сотрудников; д) найм, отбор, адаптация и мотивация сотрудников; ж) оценка личной эффективности сотрудников.3) техническое и программное обеспечение 4) разработать бизнес – план.

Используя интернет – маркетинг ИП управляет товарами на основе: 1)управления товарной номенклатурой в целом - медийная реклама; контекстная реклама; 2)оценки работы отдела, расчета стоимости продаж, регулирования издержек на продажи и управление ассортиментными группами (товарными линиями); поисковый маркетинг в целом и SEO в частности; продвижения в социальных сетях: SMO и SMM; 3) управления инновационной деятельностью - прямой маркетинг с использовании e-mail, RSS; вирусный маркетинг; 4)управления позиционированием предприятий в целом - партизанский маркетинг; интернет-брендинг.

В процессе работы ИП управляет ценами и может устанавливать: стандартные цены; престижные цены; неокругленные цены; стимулирующие цены. Для данных процессов интернет - маркетинг предлагает провести анализ цен конкурентов на основе поискового маркетинга, а также опроса покупателей с помощью e-mail, партизанского маркетинга. ИП управляет местом продажи с точки зрения следующих критериев: определение целевых клиентов осуществляется на основе «партизанского маркетинга»; управление каналами продаж, стимулирования дистрибьюторов: бонусы, акции, обучение, мерчендайзинг, с помощью телемаркетинга, дилерских и партнерских каналов продаж, рекламы, сарафанного радио. ИП управляет продвижением товара предусматривает следующие процедуры: 1) стимулирование потребителей включая премирование, демонстрации товара, усиление качества товара; 2) маркетинговые коммуникации включают рекламу, персональные продажи, паблик рилейшенз; 3) стимулирование покупателей в точках продаж: поощрение персонала, мерчендайзинг, конкурсы, соревнования. Для данных процедур ИП использует медийную рекламу, продвижение в социальных сетях с помощью SMO и SMM процедур.

Внедрение данной технологии в практику работы ИП «Тонус», показало, что конкурентоспособность ИП увеличилась, за счет использования технологий «Интернет - маркетинга»: 1) WEB – технологии http://trend-marketing.ru/mystery-shopping, модуль "Функциональный контур "Корпоративный портал" программного продукта Axapta (MicrosoftBusinessSolutions), www.axapta.sibinfo.ru. и Salesforce.com для улучшения обслуживания клиентов;2)HTML-редактора MacromediaWeb, статистических систем SPSS, Statistika, векторных графических редакторов AdobeIllustrator, CorelDraw, системырастровой графики Photoshop, создание мультимедиа презентаций MicrosoftPowerPoint, MacromediaDirector, для оптимизации и создания эффективной рекламы и продвижения продуктов;3) сайтов - информационных систем на основе HTML (HypertextMarkupLanguage) и CGI (CommonGatewayInterface) технологий поддержки работы распределённых баз данных, работающих под управлением протоколов ODBC (OpenDataBaseConnectivity), JDBC (JavaDataBaseConnectivity), которые обеспечивают обмен информацией между WEB - сервером и WEB – броузерами клиентов.

Николаев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ИНФОРМАЦИОННЫЕ РИСКИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА: АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ

Системы условного доступа (СУД) - программно - аппаратный механизм для доступа к платным кодированным цифровым, спутниковым, эфирным и кабельным телеканалам. Наиболее крупные их представители могут иметь десятки миллионов абонентов по всему миру.

В процессе работы СУД использует множество активов, в т.ч.:

- аппаратную платформу;
- программную составляющую механизма управления доступом;
- обслуживающий персонал.

Активы являются объектом для многих видов угроз. Угроза может стать причиной нежелательного инцидента, в результате которого организации будет причинён ущерб. Перечень угроз на редкость разнообразен. Сориентироваться в этом многообразии могут помочь приложения к стандартам BS 7799-3 и ISO 27005. Одно из самых детальных описаний тысяч угроз можно встретить в открытом немецком стандарте BSI IT Baseline Protection Manual.

Однако специфика функционирования СУД не отражена должным образом в существующих перечнях угроз. Существующие стандарты часто дают чрезмерно детальное описание активов и угроз, чем затрудняют применение в отношении конкретно СУД.

Целью доклада является показать примерный перечень наиболее актуальных угроз в СУД, с учётом специфики работы самой СУД.

Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОБ ОДНОМ ПОДХОДЕ К ФОРМИРОВАНИЮ СПЕЦИАЛНЫХ ДИСЦИПЛИН ВАРИАТИВНОЙ ЧАСТИ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Специалисты – выпускники уровня ВПО по роду своей деятельности, например - в процессе управления производством, всегда решают задачи, связанные с оценкой эффективности соответствующих процессов и систем (задачи анализа), а также - с формированием рациональной структуры их построения (задачи синтеза). И то, и другое, как известно, является аспектами процесса научного исследования. Поэтому, на наш взгляд, эффективное обучение в рамках высшего профессионального образования не может быть реализовано без освоения методологии научного исследования в заданной предметной области, а преподаватель высшей школы не может не быть ученым.

В связи с этим, для получения ожидаемых результатов обучения на данном уровне образования в рамках вариативной части учебного плана целесообразно, по нашему мнению, формировать и такие дисциплины, предметную область которых определяют соответствующие направления научных исследований отрасли и ВУЗа - вообще, а также - педагогического коллектива, в частности.

Так, например, подобными, органически связанными между собой направлениями НИР (и областями соответствующих научных интересов), для кафедр, связанных с применением ИТ в настоящее время соответствующих областях, на наш взгляд, являются:

- моделирование сложных организационно-технических процессов и систем;
- разработка систем интеллектуальной поддержки принятия решений в интересах управления сложными организационно-техническими системами;
- применение компьютерных технологий в НИР и учебном процессе высших учебных заведений.

Содержание некоторых результатов работы, связанной с данными направлениями деятельности, а именно: формирование предметной области и содержания дисциплины «Интеллектуальная поддержка принятия решений» и обсуждаются далее.

По поводу формирования предметной области дисциплины «Системы интеллектуальной поддержки принятия решений» следует, прежде всего, отметить, что в ее основу естественным образом могут быть положены результаты НИР кафедр в данной области. К числу таковых, например, следует отнести:

- разработка методологии построения систем интеллектуальной поддержки принятия решений (СИППР) для органов управления производством и организациями;
- экономическая и математическая постановка функциональных задач данного класса программного обеспечения (СМПО);
- формализацией решения общей и частных задач, решаемых в рамках СИППР органа управления производством или организациии;
- обоснование структуры и разработка инфологической модели информационного обеспечения СИППР;
- разработка методов рационального управления ресурсами и методик их реализации.

При этом данные исследования могут базироваться, на наш взгляд, на следующей концептуальной трактовке понятий информационной системы и СИППР.

С точки зрения реализации своих функций процесс управления носит явно выраженный информационный характер (обработка данных в интересах получения новых сведений) о состоянии управляемого объекта и выработки новых управляющих воздействий.

В связи с этим, в структуре любой системы управления может быть выделен такой функциональный элемент, назначение которого состоит в том, чтобы реализовать ее функции учета и

анализа (по результатам обработки имеемых данных обеспечить поддержку принятия органами управления наиболее целесообразных решений.

В качестве такого функционального элемента систем управления чаще всего определяют их информационные подсистемы (или ИС в случае их рассмотрения как самостоятельного объекта), реализующие на практике применение, как правило, новых (компьютерных) технологий.

В тоже время, рассматривая многообразие существующих в н.в. ИС с точки зрения их возможностей поддерживать решения (или соответствующей степени делегирования им таковых полномочий), а также механизмов их реализации можно утверждать, что системам поддержки принятия решений (СППР) - Decision Support Systems (DSS). следует называть - специализированные варианты построения ИС, обеспечивающие реализацию процедур (бизнес-правил) обработки данных или знаний в интересах анализа эффективности процессов в соответствующих предметных областях и синтез тех систем, в которых они реализуются.

Останина М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ФРЕЙМВОРК УПРАВЛЕНИЯ БИЗНЕС-ИНФОРМАЦИЕЙ BISL

Изучение методологии Фреймворка BISL (Business Information Services Library), ориентированного на реализацию процессов и эталонных моделей управления бизнес-информацией, способствует повышению эффективности бизнеса. Актуальность данной методологии объясняется возросшей необходимостью управления информацией не только на стороне Поставщика, но и на стороне Заказчика ИТ-услуг. Большую роль в применении Фреймворка BISL играет передовой опыт, согласующийся со структурой методологии и учитывающий специфику предметной деятельности организации. Рекомендации к построению бизнес-процессов, в частности модель BISL, способствуют стандартизации и повышению качества информационного обеспечения и выявлению рисков, что является конечной целью использования Фреймворка управления бизнес-информацией.

Соколов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА

Рассматривается принципы построения моделей управления информационными рисками в системах условного доступа (СУД). Назначение моделей состоит в обоснованном выборе вариантов организации системы противодействия информационным атакам на СУД, представляющих собой набор мероприятий противодействия атакам. В качестве критериев и ограничений моделей используются значения вероятностей взлома СУД и нарушения обслуживания абонентов за определенный интервал времени и величина совокупной среднегодовой стоимости владения системой обеспечения информационной безопасности.

Предлагается совокупность принципов построения моделей. Специфическими принципами построения моделей являются:

а) адекватность параметров моделей особенностям управления информационными рисками СУД;

б) выбор временного интервала, соответствующего учету вероятности не более чем однократной атаки;

в) классификация атак по признаку однородности,что позволяет установить однозначность выбора противодействующих мероприятий для каждого вида атак;

г) однократность затрат на защитное мероприятие при его многократном использовании для противодействия разным видам атак.

Предлагается три модели условной оптимизации и модель безусловной оптимизации системы защиты СУД от информационных атак, представляющие собой модели линейного программирования с двоичными переменными.

Модель условной оптимизации совокупной среднегодовой стоимости владения системы управления информационными рисками предполагает наличие ограничений на вероятность возникновения рискового события, связанного со взломом СУД и вероятность нарушения обслуживания абонентов СУД на протяжении выбранного интервала времени.

На основе данной модели можно предложить две взаимно обратные задачи оптимизации, в которых критерий и ограничения меняются местами.

В модели безусловной оптимизации отсутствуют условия соблюдения допустимых вероятностей возникновения рисковых событий, связанных со взломом и нарушением обслуживания абонентов СУД.

Вместо этих условий в целевую функцию минимизации совокупной среднегодовой стоимости владения системой управления информационными рисками СУД добавляются значения математических ожиданий среднегодовых затрат при возникновении рисковых событий.

В моделях присутствуют два вида двоичных переменных, одна из которых характеризует использование в системе мероприятий, противодействующих атакам, а другая – привязку этих мероприятий к атакам различного вида. Такой подход обеспечивает однородность учета затрат на каждое мероприятие при его многократном использовании для противодействия атакам различного вида. Эти модели могут быть решены с помощью ряда известных математических программных пакетов, например, MATLAB.

Тюрликов А.М., Татарникова А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

СИСТЕМА ОБНАРУЖЕНИЯ ПАТОЛОГИЙ ОПОРНО-ДВИГАТЕЛЬНОГО АППАРАТА С ПОМОЩЬЮ АКСЕЛЕРОМЕТРОВ МОБИЛЬНЫХ УСТРОЙСТВ

Актуальность работы обусловлена исследованием возможностей использования акселерометров мобильных устройств для обнаружения патологий опорно-двигательного аппарата человека (ОДА).

Идея основана на оценки функционального состояния ОДА применением информативных параметров. Известно, что при возникновении заболевания ОДА в частотном спектре возможны изменения, например, появление пиков на высоких частотах. Таким образом, по походке человека, применяя мобильное приложение, фиксирующее показания акселерометра в мобильном телефоне, можно обнаруживать патологии ОДА и отправлять соответствующие данные лечащему врачу.

Для проверки данного предположения был проведен ряд экспериментов, суть которых заключалась в следующем:

- мобильный телефон фиксировался на теле человека, после чего испытуемый в течение, приблизительно, 15 с должен был пройти по прямой своей обычной походкой. За это время происходила запись данных с трех осей акселерометра. Отсчеты брались с частотой 100 Гц (каждые 10 мс);
- данные с акселерометра подвергались дискретному преобразованию Фурье (ДПФ);
- полученные спектры анализировались на качественном уровне.

В эксперименте участвовало 13 человек. В результате проведенных испытаний выявлены следующие типовые особенности в спектрах:

1. Максимальные амплитуды колебаний по всем осям акселерометра у большинства испытуемых находятся на одних и тех же частотах.

2. У большинства испытуемых наиболее сильные колебания происходят по направлению вверх-вниз.

3. С возрастом у человека появляются более сильные высокочастотные составляющие в спектре вне зависимости от наличия заболеваний ОДА.

Характерные особенности в спектрах были выявлены у двоих испытуемых: у одного (21 год, пол – м, заболевание ОДА – сколиоз третьей степени) выявлен максимум колебаний по направлению вперед-назад смещен в область высоких частот, а у другого (80 лет, пол – м, заболевание ОДА – коксартроз) выявлена более высокая амплитуда колебаний в направлении вправо-влево.

Хамхоева Х.М., Абрамян Г.В.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации, Российский государственный педагогический университет им. А. И. Герцена, Санкт-Петербургский государственный институт психологии и социальной работы

ИНФОРМАЦИОННАЯ МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ НАВИГАЦИИ МАРШРУТОВ ПОИСКА, ДИСТАНЦИОННОГО КОНСУЛЬТИРОВАНИЯ И ПОКУПОК ТОВАРОВ НАРОДНОГО ПОТРЕБЛЕНИЯ

В информационном обществе (ИО) около 75 % товаров народного потребления (ТНП) ориентированы на удовлетворение «модных» или «трендовых» потребностей людей. Однако В условиях падения курса рубля при покупке одежды в магазинах по низким и «доступным» ценам у студентов и школьников в РФ возникают жалобы на:

1) низкое качество приобретенных вещей;
2) ограниченность цветовой гаммы;
3) отсутствие разнообразия в моделях;
4) отсутствие нужных размеров;
5) необходимость выбора между комфортом и красотой;
6) недостатки одежды для деловых встреч;
7) недостатки комплектов одежды;
8) плохое сочетание стилей.

В связи с этим студенты, школьники и их родители тратят все больше времени и ресурсов на поиск качественных, но доступных товаров, посещая различные магазины и торговые центры.

В статье предлагается модель интеллектуальной системы навигации маршрутов поиска, дистанционного консультирования и покупок ТНП для студентов и школьников РФ включающая:

1. систему обучения покупательству (шопингу) на основе On-line консультирования покупок и продаж ТНП;

2. систему финансового анализа покупок и продаж ТНП на основе агентных On-line сервисов. Для реализации модели предлагается спроектировать учебно-познавательный сайт-ресурс, на котором будут размещены материалы для эффективной покупки и продажи одежды: 1) рекомендации по предметам гардероба студентов и школьников с учетом региона, времени года (сезона), бюджета и времени; 2) методические рекомендации по формированию умений расчета бюджета покупок; 3) уроки-практикумы по типовым ситуациям покупок в торговых центрах и On-line продаж.

В систему Shoping On-line навигации маршрутов поиска и дистанционного консультирования шопинга будут заложены адаптивные технологии расчетов маршрутов в зависимости от различных критериев: 1) наиболее оптимальный (короткий) маршрут по расстоянию, 2) наиболее оптимальный (короткий) маршрут по времени, 3) наименьшие затраты финансовых средств, 4) высокое (среднее, низкое) качество покупок, 5) высокое (среднее, низкое) качество обслуживания и сервиса, 6) высокая (средняя, низкая) надежность продавца (покупателя) и др.

В основу интеллектуальной системы навигации Shoping On-line будут заложены принципы интерактивной организации визуальной и вербальной информации: 1) достоверность и непрерывность, которые обеспечат адекватность информации текущему, фактическому положению и ситуации на рынке ТНП; при этом непрерывность обеспечит постоянность поступления информации на всём маршруте движения ИА-покупателя от начальной до конечной его точки маршрута в любой момент времени по пути его следования, 2) точность и актуальность обеспечат однозначность информационных сообщений, не допуская различных толкований, 3) необходимость и достаточность обеспечат максимальные сведения и данные, необходимые покупателю на всем маршруте следования, причем текстовые сведения, дизайн оформления (цвет, шрифт и др.) и графические данные товара не должны мешать восприятию визуальных характеристик общей навигационной информации; 4) единообразие и универсальность обеспечат представление и функционирование визуальной и вербальной информации совместно с другими системами навигации, например навигационными сервисами цифровой картографии Навител Навигатор автомобильных GPS систем, онлайн-сервисов: Навител. Пробки, Навител. Друзья, Навител. События, динамических POI, Навител. SMS, Навител. Погода.

Результатом внедрения будет интеллектуальная система навигации маршрутов и дистанционного консультирования с учетом сведений, как о товарах, так и о торговых центрах: планов-схем этажей, указателей, предупреждающих знаков, таблиц, пиктограмм, вывесок, выставочных стендов, активных элементов (гербов, логотипов, макетов, муляжей), которые позволят студентам, школьникам и их родителя ориентироваться в пространстве ТНП.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИНАНСОВО-КРЕДИТНОЙ СФЕРЫ И БИЗНЕСА

Алмаметов Т.Г., Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ В ПРИЛОЖЕНИЯ ПОД ANDROID

Активный рост количества используемых мобильных устройств и их функциональных возможностей привел к появлению новых видов вредоносных программ. К их числу можно отнести:

- различные программы - вымогатели, которые блокируют доступ к устройству и требуют от владельца устройства перевода денежных средств;
- многочисленные мобильные вирусы;
- вредоносные мобильные приложения, которые способны похитить банковскую или другую конфиденциальную информацию;
- SMS - трояны, которые рассылают от имени пользователя нежелательную информацию и др.

В 2015 году на различных мобильных платформах по отчёту АО «Лаборатории Касперского» было обнаружено около трёх миллионов инсталляционных пакетов, содержащих вредоносный код, из которых треть - недавно созданное вредоносное программное обеспечение. С каждым годом число новых опасных приложений увеличивается.

Магазины приложений (в т. ч. Google Play Market) играют важную роль в популярности смартфонов и планшетов, использующих ту или иную платформу (Android). Открытость этих магазинов приложений делает их большой мишенью для создателей вредоносного программного обеспечения.

Среди операционных систем для мобильных телефонов, наибольшей популярностью пользуется Android. Компания Google отреагировал на рост числа потенциально опасных приложений, начав использовать Bouncer - сервис, который проверяет приложения, отправленные на публикацию в Play Store.

В настоящее время основным защитным механизмом, доступным пользователю является механизм разрешений. Этот механизм далеко не идеален. Основная проблема заключается в том, что пользователю нужно обладать определёнными техническими знаниями, чтобы иметь возможность отличить вредоносное приложение от безвредного приложения. Отдельные разрешения дают разработчику приложения доступ к ряду возможностей, лишь часть из которых может потенциально быть использована для нанесения вреда. Поэтому вредоносные и безвредные приложения могут запрашивать одинаковые разрешения и быть неразличимы лишь с использованием механизма разрешений.

Работа антивирусов и систем обнаружения вредоносной активности в основном строится на использовании базы сигнатур известных зловредов. Если было найдено соответствие какого-либо участка кода известной сигнатуре, то антивирусная программа может удалить или попытаться восстановить файл.

Подобный метод обнаружения требует наличие часто и своевременно обновляемых баз сигнатур. Сигнатуры, в свою очередь, создаются в результате анализа вируса вручную. Возможность автоматизации процесса создания сигнатур была многократно исследована и признана проблемной, плохо поддающейся автоматизации.

Приложения под Android могут быть легко декомпилированны, что означает, что приложения легко модифицируются и могут быть перепакованы. Изменится и сигнатура приложения. Этой особенностью активно пользуются создатели вредоносных приложений, внедряя код в приложения вызывающие у пользователей доверие.

Антивирусные программы, созданные на основе метода поиска сигнатур, могут эффективно препятствовать вспышкам вирусов. Однако, авторы вирусов могут создать полиморфический вирус, в котором части кода модифицируются, шифруются и/или искажаются, чтобы невозможно было обнаружить совпадение с уже найденным вирусом в базе сигнатур. Также к недостаткам методов обнаружения, основанных на сигнатурах, можно отнести - необходимость регулярного и оперативного их обновления, трудоемкость ручного анализа, отсутствие возможности выявить какие-либо новые виды атак.

Поэтому требуется использование другого более совершенного механизма для поиска вредоносной активности, желательно в автоматическом режиме. И в этом качестве возможности машинного обучения могут помочь в решении столь сложной задачи.

Целью проводимой работы являлось создание средства для осуществления автоматизированной классификации приложений Android OS на безвредные и потенциально опасные с использованием методов машинного обучения.

При использовании методов машинного обучения основной упор сделан на выявлении особенных характеристик и черт приложений, с помощью которых можно классифицировать с большой вероятностью наличие потенциальных угроз со стороны приложения. При этом такой подход одинаково хорошо работает как для уже известных видов угроз, так и для новых.

Создаваемое решение должно уметь:

- Анализировать приложение по запросу пользователя на наличие потенциальной угрозы;
- Создавать отчёт о найденных потенциальных угрозах;
- Вносить правки и модификации в модель машинного обучения;
- Осуществлять проверку моделей машинного обучения на тестовом наборе приложений;
- Обеспечивать взаимодействие с пользователем через графический пользовательский интерфейс.
- Для создания программного решения, способного выполнять описанные выше операции, необходимо осуществить ряд действий:
- Выделить признаки, которые должны быть использованы для выявления угрозы со стороны приложения;
- Создать приложение, которое будет извлекать признаки;
- Реализовать модель машинного обучения, способную по извлечённым признакам осуществить анализ приложения;
- Обеспечить возможность модификации модели машинного обучения;
- Создать базу данных для хранения информации о результатах анализа приложений;
- Разработать интерфейс для взаимодействия с пользователем.

Для осуществления классификации использованы следующие две группы признаков:

- Запрашиваемые приложением разрешения (файл манифеста, который доступен вместе с приложением);
- Потенциально опасные вызовы, совершаемые приложением (известная база инцидентов).
- Для работы всех частей предложенного программного решения был использован следующий инструментарий:
- Android Asset Packaging Tool – инструмент используемый во время сборки приложений под Android OS. Входит в состав Android SDK;
- 7-Zip – открытое программное обеспечение для работы с архивами;
- Java SE Runtime Environment – минимальная реализация виртуальной машины, необходимая для исполнения Java-приложений, без компилятора и других средств разработки;
- baksmali.jar – дизассемблер для формата dex, используемого виртуальной машиной Dalvik;
- Tensorflow – библиотека для машинного обучения;
- Python 3 – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода.

Разработанное программное решение подтвердило то, что использование методов машинного обучения для определения вредоносных приложений является реализуемой задачей и может быть достаточно эффективно использовано для проверки приложений на наличие потенциально вредоносного поведения.

Аминова Х.И., Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ГИБРИДНОЙ ОБЛАЧНОЙ ПЛАТФОРМЫ ДЛЯ ОРГАНИЗАЦИИ СОВРЕМЕННОЙ БАНКОВСКОЙ ИТ-ИНФРАСТРУКТУРЫ

Современный банк невозможно представить без современной, эффективной, надежной и масштабируемой ИТ-инфраструктуры, который влияет на стратегическую и операционную эффективность.

ИТ-инфраструктура создает основу информационного обеспечения банка, что позволяет обеспечить сотрудников и клиентов оперативными и достоверными информационными и интеллектуальными ресурсами, необходимые для объективного анализа, оценки и прогноза развития банковского бизнеса.

Требования к банковской ИТ-инфраструктуре во многом схожи с любыми развивающимися и высокотехнологичными компаниями, такие как: минимизация издержек, необходимость привлечения большего количества клиентов, увеличение пропускной способности транзакционных систем,

снижение времени доступа к информации, необходимость получения информации в реальном времени и т.п.

При построении ИТ-инфраструктуры традиционно используются: стандарт ИСО 20000, ITIL, библиотека ITSM (издаваемая itSMF), методология MOF от компании Microsoft, универсальный свод знаний по управлению услугами (USMBOK), COBIT и др.

Задача создания банковской ИТ-инфраструктуры заключается в формировании таких условий ее функционирования, которые способны обеспечить эффективность и надежность банковского бизнеса.

Основной тенденцией построения современной банковской ИТ – инфраструктуры является рост интереса к виртуализации и использованию облачных технологий с той оговоркой, что отличительной особенностью банковской ИТ-инфраструктуры являются более высокие требования к безопасности и надежности, в том числе со стороны Банка России, например, СТО БР ИБСС.

Многочисленные эксперты отмечают, что

- использование публичных облачных сред для осуществления банковской деятельности не получило распространения из – за проблем с безопасностью данных;
- а использование частного облака требует создание или аренду локального ЦОДа, соблюдение ряда требований по необходимости размещения информации, содержащей персональные данные на территории РФ.
- все чаще звучат мнения о целесообразности создания гибридной банковской ИТ-инфраструктуры.

Облачные технологии базируются на сервис-ориентированной архитектуре и технологии виртуализации. Применяя облачные технологии, банк может либо создать частные облака, либо «арендовать» вычислительную мощность или серверы, оплачивая их использование по времени. Среди решений, позволяющие создавать частные облака можно отметить программно-аппаратные комплексы HP CloudMatrix, IBM Cloud Burst, vBlock, VMWare vCloud Director и др.

Публичные облака не востребованы банками из-за безопасности данных. Использование публичного облака не позволяет обеспечить безопасность данных в полном объеме. Альтернативой может служить использование гибридных облаков.

При использовании гибридных облаков, которые сочетают особенности совместного использования частных и публичных облаков, возможно обеспечение необходимого уровня информационной безопасности, «цифрового суверенитета» (облачные технологии в большинстве не российской разработки) и ряда требований ФЗ «О персональных данных» (необходимость хранения данных в ЦОДах на территории РФ).

Поэтому необходимо исследовать возможность построения гибридного решения на существующих облачных платформах, провести технико-экономическое обоснование целесообразности создания подобного решения. В процессе исследования необходимо провести классификацию требований и ожиданий российских банков от подобного решения.

Появляется актуальная задача выбрать из многообразия облачных технологий для построения гибридного облачного решения наиболее подходящего. Проведенный анализ рынка программного обеспечения выявил появление предварительной версии новой гибридной облачной платформы Microsoft Azure Stack! и стало возможным проверка гипотезы о возможности и целесообразности развертывания гибридного облачного решения для организации полноценной банковской ИТ-инфраструктуры.

Ожидается, что данное решение окажется сбалансированным и будет подходить для большинства заинтересованных участников рынка, как по цене, так и по функциональным возможностям.

Богатырев В.А., Паршутина С.А., Попцова Н.А.
Россия, Санкт-Петербург, Университет ИТМО

ИМИТАЦИОННАЯ МОДЕЛЬ СЕТИ С МНОГОПУТЕВОЙ РЕЗЕРВИРОВАННОЙ МАРШРУТИЗАЦИЕЙ

Для распределенных систем с многопутевой маршрутизацией, увеличение вероятности безошибочной доставки пакетов за ограниченное время может достигаться при резервированной передаче копий пакетов по нескольким маршрутам.

При необходимости доставки хотя бы одной копии, своевременность и безошибочность доставки пакетов адресату возможна без использования протоколов подтверждений и повторных передач. Вместе с тем, резервированная передача копий пакетов приводит к увеличению суммарной интенсивности передач, а поэтому может вызвать увеличение задержек доставки копии. В тоже время из-за стохастичности независимой передачи копий пакетов по разным каналам вероятность своевременной доставки хотя бы одной передаваемой копии может возрасти, что, при определенных условиях, может привести к уменьшению среднего времени ожидания (пребывания) запросов в системе.

Исследование интегрированной эффективности многопутевой передачи копий запросов через сеть и их резервированного обслуживания в кластере на основе аналитического моделирования достаточно трудоемко, что обусловливает целесообразность имитационного моделирования исследуемых систем.

В качестве объекта исследования рассматриваются группа серверов, объединяемых в кластер с целью резервированного обслуживания копий запросов, поступающих через многоуровневую сеть. Резервированное обслуживание и доставка через сеть к серверам копий запросов реализуется для обеспечения безошибочного и своевременного обслуживания хотя бы одной из создаваемых резервных копий запросов. Рассмотрены случаи, когда в распределенной системе поддерживается резервированная передача пакетов по k из m возможным путей на один сервер (узел), либо на k из n серверов кластера. Запрос считается успешно выполненным, если хотя бы одна из k его копий будет безошибочно доставлена в сервер готовый к ее обслуживанию и при этом, хотя бы один из принятых к обслуживанию запросов будет безошибочно выполнен в установленный срок.

Целью работы является создание имитационных моделей и средств поддержки проектирования высоконадежных распределенных систем. Создаваемые модели предназначены для анализа эффективности и выбора наилучших вариантов проектных решений по построению сетей с резервированной передачей и обслуживанием запросов.

Разрабатываемые имитационные модели исследуемой распределенной системы строятся в среде имитационного моделирования AnyLogic 7. Исследования направлены на оценку эффективности и целесообразности резервированной доставки через сеть копий запросов и их резервированного обслуживании в узлах кластера.

При построении модели считается, что в сети реализуется доставка копий запросов к серверам кластера по непересекающимся путям, возможно различным по числу узлов, задействованных при передаче копий запросов.

Показана эффективность резервированной передачи копий запросов (пакетов) к серверам кластера по нескольким путям с резервированным независимым обслуживанием копий запросов группой серверов кластера. Это позволяет увеличить вероятность безошибочного выполнения хотя бы одной копии запроса в установленные сроки, что позволяет рекомендовать предлагаемые решения для систем, работающих в реальном времени.

Богатырев В.А., Сластихин И.А.
Россия, Санкт-Петербург, Университет ИТМО

МЕЖМАШИННЫЙ ОБМЕН В РЕАЛЬНОМ ВРЕМЕНИ ЧЕРЕЗ РЕЗЕРВИРОВАННЫЕ КАНАЛЫ

Высокие требования к надежности, отказоустойчивости, информационной безопасности, и пропускной способности инфрокоммуникационных систем и сетей достигаются при резервировании и агрегировании каналов связи.

В системах с агрегацией каналов повышение надежности доставки пакетов адресату возможно в результате резервированной передачи копий пакетов через несколько каналов. За основу резервированной передачи копий пакетов может быть взяты дисциплины резервированного обслуживания запросов. Передача резервных копий пакетов по разным каналам направлена на повышение вероятности их безошибочной доставки адресату при ограничении допустимых задержек, что важно для систем реального времени.

В качестве альтернативного варианта, направленного на повышение надежности передачи в сети, рассмотрим организацию межмашинного обмена при объединении агрегированных каналов в группы, когда каждый вычислительный узел сети подключен к агрегированным каналам, разделенным на группы. Для запросов на передачу пакетов организуется общая очередь. В результате множественного доступа по каждому запросу одновременно предоставляются ресурсы всех каналов одной из групп. При предоставлении узлу доступа к группе каналов, пакет из его общей очереди копируется. После чего каждая резервная копия пакета передается через отдельный канал группы. В результате такой организации осуществляется резервированная передача копий пакета (запроса). Ввиду идентичности каналов и одновременного их предоставления для передачи пакета, считаем, что все копии будут доставлены адресату одновременно, хотя при этом возможна передача с ошибками или потеря пакетов. Резервированная передача пакетов позволяет увеличить вероятность безошибочности доставки адресату хотя бы одной копии пакета и снизить издержки повторных перечах ошибочно доставленных пакетов. Вместе с тем, передача копий пакетов увеличивает нагрузку агрегированного канала и может привести к увеличению времени пребывания пакетов в системе и в итоге к возможному снижению вероятности доставки пакетов за предельно допустимое время. Указанное техническое противоречие обусловливает необходимость определения области (границы) эффективного резервирования передач копий пакетов через агрегированные каналы.

Целью исследования является определение границ целесообразного применения резервированной передачи пакетов, критичных к времени их безошибочной доставки через агрегированные каналы, объединяемые в группы.

При передаче пакетов через агрегированные каналы очереди отдельных узлов объединяются в общую очередь по реализации множественного доступа к резервированным группам каналам. При этом, если пренебречь задержками на организацию множественного доступа, то система представляется, как многоканальная система массового обслуживания с общей очередью. Ввиду идентичности каналов и одновременности передачи по *k* каналам одной группы резервных копий пакетов каждую группу каналов представим в виде одного обслуживающего прибора.

В результате расчетов показана эффективность организации резервированных передач копий пакетов через агрегированные каналы, разделенные на группы. Определены границы целесообразного применения резервированной передачи пакетов, критичных к времени их безошибочной доставки через агрегированные каналы, разделяемые на группы

Власова И.А.
Россия, Санкт-Петербург, Северо-Западный институт управления РАНХиГС

ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СУБЪЕКТОВ ВОЕННО-ТЕХНИЧЕСКОГО СОТРУДНИЧЕСТВА СО СТРАНАМИ СНГ

В соответствии с законом Российской Федерации военно-техническое сотрудничество (ВТС) представляет собой деятельность в области международных отношений, связанная с вывозом и ввозом, в том числе с поставкой или закупкой, продукции военного назначения, а также с разработкой и производством продукции военного назначения. Роль ВТС в экономике страны постоянно возрастает и в настоящее время приближается к роли торговли энергоносителями. Одним из основных факторов в повышении эффективности субъектов ВТС лежит их информационное обеспечение, которое представляет собой совокупность информационных ресурсов и услуг, предоставляемых для решения управленческих и научно технических задач в соответствии с этапами их выполнения. Среди множества задач, решаемых в процессе ВТС важнейшее место занимает задача разработки концептуальных подходов к решению проблемы повышения его эффективности, а также задача анализа тенденций развития рынков продукции военного назначения в государствах и регионах ведения.

В зависимости от специфики государств и региона сотрудничества информационное обеспечение ведения ВТС имеет свои особенности. Они связаны, во-первых: с характером используемой информации; во-вторых, с методами ее добывания.

К числу основных особенностей ВТС со странами СНГ (Азербайджан, Армения, Белоруссия, Казахстан, Кыргызстан, Молдова, Таджикистан, Узбекистан) можно отнести следующие.

1. Использование информации по меньшей мере трех типов:

– информацию политико-экономического характера, к которой можно отнести сведения о состоянии вооруженных сил СНГ; об экономических возможностях этих государств; о взаимоотношениях этих государств с сопредельными государствами, государствами региона и мира в целом; о состоянии нормативно-законодательной базы в различных сферах жизни (в первую очередь информационной) России и государств взаимодействия и т.п.

– информацию военно-технического характера, к которой можно отнести сведения о имеющемся вооружении и военной техники; о наличии ремонтной и обслуживающей базы; о наличии квалифицированных специалистов в области современных средств вооруженной борьбы, и т.п.;

– информацию прогнозного характера, например о потенциальной востребованности государств взаимодействиях в инновационных разработках предприятий российского оборонно-промышленного комплекса; о перспективах маркетинговой, рекламной, рекламно-выставочной деятельности в области ВТС и т.п.

2. Основной особенностью получения большинства информации военно-технического и прогнозного характера при ведении ВТС со странами СНГ является необходимость ее получения только методами, соответствующими действующим законодательствам сотрудничающих государств, то есть специальными методами промышленного маркетинга (деловой разведки). Другая информация может быть получена по линии взаимодействия от различных государственных органов, в первую очередь осуществляющих международную деятельность и других официальных структур.

Практическая реализация эффективного информационного обеспечения потребует создания в организационных структурах субъектов ВТС специальных подразделений деловой разведки, осуществляющих добывание (сбор) и обработку необходимой информации, а также подготовку специалистов в области информационно-аналитической работы по данному направлению.

Гончаров В.В.
Россия, Санкт-Петербург, ООО «МЭС»

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОЙ ПЕРЕПИСКЕ ПРЕДПРИЯТИЙ

Электронная подпись представляет собой определённую электронную информацию обозначающую подпись, которая увязывается с другой, подписываемой электронной информацией и

используется для определения личности подписавшего. Существует два вида электронных подписей. простая и усиленная. Информация простой электронной подписи состоит из имени пользователя и пароля. Простая электронная подпись малопригодна для бизнес-коммуникаций, так как её трудно защитить от утечки. Поэтому в рамках темы доклада речь будет идти преимущественно о технологии усиленной электронной подписи. Такая электронная подпись предполагает наличие в стране определённой инфраструктуры, обеспечивающей выдачу инструментов электронной подписи и контролирующей процесс их использования. Выполнение этой функции осуществляют так называемые удостоверяющие центры – аккредитованные государством частные или государственные организации, обеспечивающие создание и выдачу ключей проверки электронной подписи. Ключ проверки электронной подписи - это инструмент проверки подлинности электронных подписей, имеющий электронную форму. Указанная инфраструктура содержит специальные шифровальные (криптографические) средства, которые могут осуществлять различные функции: создание электронной подписи; проверка электронной подписи; создание ключа электронной подписи и ключа проверки электронной подписи. Разные организации могут кооперативно выполнять отдельные функции или все из них.

В России электронная подпись была признана федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ, что способствовало широкому распространению этой технологии в практике бизнес-коммуникаций отечественных предприятий. В настоящее время вся отчётность по налогу на добавленную стоимость успешно сдаётся и принимается в электронной форме, которая предполагает применение электронной подписи. В этой связи целесообразно рассмотреть перспективы развития практики применения электронной подписи в отношениях предприятий не только с государственными органами, но и с другими контрагентами (поставщиками, заказчиками, покупателями).

Обычным для современного рынка средством бизнес-коммуникаций стала интернет-переписка. При этом интернет переписка может иметь юридическое значение, быть доказательством в суде. Вместе с тем, существуют большие трудности в определении судом достоверности переписки, если сторона её отрицает. Кроме того, специальные мероприятия по нотариальному заверению переписки обычно являются дорогостоящими, а принятие её судом в качестве доказательства не гарантирована. Существенной проблем является также то, что плохо определённый юридический статус электронной переписки подчас используется мошенниками, злоупотребляющими доверием своих жертв к электронным письмам. Исправление недостатков электронной переписки в бизнесе, связано на наш взгляд с совершенствованием законодательства. Раньше, пять лет назад, индустрия, обеспечивающая электронную подпись, была менее развитой, и возможно, поэтому закон не мог требовать обязательности электронной подписи для любой электронной переписки в бизнесе. Однако в настоящее время электронная подпись применяется практически всеми предприятиями, и многие граждане пользуется ею для получения государственных услуг. Поэтому в качестве перспективной меры государственного регулирования рекомендуется следующее:

1. обязать суды принимать в качестве доказательства только те электронные письма, которые заверены электронной подписью, по любым делам, связанным с совершением сделки;

2. обязать предприятия использовать электронную подпись в электронной переписке по поводу любой сделки;

3. обязать применять электронную подпись всеми сторонами, если договор между ними предполагает ведение электронной переписки.

Вместе с тем следует учесть негативный сопутствующий эффект предложенных мер, который будет выражаться в развитии способов подделки электронной подписи. Сегодня наиболее действенным методом подделки является получение двух документов с одинаковой подписью. Данный метод использует недостатки алгоритмов программ, обеспечивающих электронную подпись. Необходимо предусмотреть растущие возможности ЭВМ и ориентироваться на создание неуязвимой системы электронной подписи, возможно с использованием видеокамер и сенсорных устройств, подтверждающих личность, место и время совершения электронной подписи.

Гончаров В.В.
Россия, Санкт-Петербург, ООО «МЭС»

ЗАДАЧИ РАЗВИТИЯ ВАЖНЕЙШИХ СИСТЕМ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ РОССИЙСКОЙ ЭКОНОМИКИ

Научно-техническая революция в области информационных технологий в 1970 годы, а также последующее за ней развитие и удешевление производства компьютерной техники обеспечили массовое распространение персональных компьютеров, сети Интернет и банковских карт, начинавшееся во второй половине 1990-х годов. В настоящее время компьютерные приложения позволяют автоматизировать любые трудоёмкие процессы, связанные с математическими вычислениями и обработкой информации, сокращая затраты времени специалиста на работу и

обучение профессии. Компьютерные приложения интегрированы не только в отечественный бизнес, но и в деятельность учреждений и органов государственной власти.

Вместе с тем компьютерные приложения в большинстве своём работают в операционной системе Windows, которая принадлежит американской корпорации Microsoft. Данная зарубежная корпорация вправе по своему усмотрению прекратить распространять эту операционную систему. Такой шаг корпорации сделает невозможным установку большинства компьютерных приложений на новые компьютеры, в которых нет соответствующей операционной системы или на компьютеры с истекшей лицензией на использование Windows. Особую актуальность данная проблема приобретает в связи с практикой санкций в отношении России со стороны западных государств и поддерживающих их зарубежных частных компаний. Компьютерные приложения, не работающие без Windows, обслуживают практически все отрасли народного хозяйства страны, поэтому риски, связанные с возможным решением американской корпорации имеют стратегическое для России значение. Достижение цели независимости государства от корпораций, производящих операционные системы (Microsoft, Linux) предполагает, на наш взгляд, меры нормативно-правового характера и/или разработку «национальной» операционной системы, по аналогии с создаваемой сейчас национальной платёжной системой. В частности, органам государственной власти целесообразно заблаговременно рассмотреть возможность временной легализации применения нелицензионных операционных систем в том случае, если отзыв лицензии правообладателем может нанести большой ущерб российской экономике. Аналогичная мера может быть применена в отношении монополистов на рынке бухгалтерских программ и любых других стратегически значимых компьютерных приложений. Следующая мера нормативно-правового характера - обязать безвозмездно предоставлять государству бессрочную лицензию на стратегически значимое компьютерные приложения, что будет служить гарантией стабильности экономики в случае ухода правообладателя с российского рынка. Такая лицензия должна распространяться на всех граждан в случае, если производитель или правообладатель решит прекратить продавать или поддерживать программное приложение, важное для экономики страны или региона. Особенности «национальной» операционной системы должны зависеть от решения судебной власти по вопросу легализации компьютерных приложений. В случае признания судебной властью конституционности закона о легализации нарушения лицензии при определённых условиях, «национальная» операционная система должна быть совместима с наиболее распространёнными операционными системами и программными приложениями, которым присвоен статус «стратегических», а интерфейс необходимо максимально приблизить к привычным для большинства граждан формам, чтобы минимизировать затраты времени и бюджета на переобучение. До начала реализации предложенной идеи потребуется на основании референдума отменить верховенство международных норм над национальным законодательством, поэтому рассмотренная мера рассчитана на длительное и постепенное продвижение к стратегической цели независимости информационной системы экономики страны.

Другой потенциальной стратегической угрозой системе информационного обеспечения экономики России является отключение страны или её региона от глобальной сети Интернет. Инициатива ограничения сети Интернет в стране или в регионе может исходить от органов государственного управления, например, в интересах или под предлогом борьбы с терроризмом. Учитывая исключительно важную роль, которую глобальная сеть Интернет приобрела за последние 15 лет в России для большинства граждан, целесообразно в конституции закрепить их право на свободное использование Интернетом и запретить оперативное отключение или ограничение интернета на всех уровнях власти. В свете участившихся обвинений российской власти в хакерских атаках нельзя исключать возможность будущих угроз отключить Россию от сегмента сети Интернет США и западных государств. В виду этого государству рекомендуется поощрять развитие интернет-технологий, затрудняющих ограничения извне, а также средств преодоления таких ограничений.

Таким образом, основные задачи государства по развитию стратегически важного информационного обеспечения экономики России состоят в превентивной защите экономики от возможного произвола правообладателей-монополистов, а решение этих задач требует конституционных реформ, отвечающих новым ценностям современного информационного общества.

Горенбургов М.А., Гончаров В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения, ООО «МЭС»

ЭВОЛЮЦИЯ БУХГАЛТЕРСКИХ ПРОГРАММ КАК ОБЪЕКТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ

Бухгалтерский учёт является одной из основ функционирования всех организаций в современном мире, обеспечивая государству сбор и обработку информации об их деятельности по установленным правилам. В этой связи в России насчитывается до пяти миллионов бухгалтеров (по данным Российский союз промышленников и предпринимателей, 2013 г.). Сегодня деятельность всех бухгалтеров обязательно связана с применением бухгалтерских компьютерных приложений, так как с

2016 года все плательщики налога на добавленную стоимость (НДС) должны представлять налоговую отчетность в электронном виде. Отчётность по налогу на доходы физических лиц (НДФЛ) и отчёты в Пенсионный фонд РФ (ПФР РФ) также сдаются по сети интернет, но в отличие от отчёта НДС, это обязательно для организаций с численностью работников свыше 25 человек. На практике же большинство даже малых предприятий сдают в электронном виде отчетность не только НДС, но и НДФЛ, ПФР, ФСС (фонд социального страхования), так как это обычно входит в базовый пакет услуг организаций-операторов, отвечающих за передачу отчётов с рабочего места в налоговую инспекцию, ПФР, ФСС. Кроме того, в течение нескольких лет до 2016 года отчёты в налоговую инспекцию и в ПФР должны были сдаваться в электронном виде на дискете или карте флеш-памяти с приложением бумажных копий отчёта. Автоматизация и механизация процесса сдачи-приёма отчётности на государственном уровне стала возможна благодаря тому, что ведение бухгалтерского учёта в электронном виде широко внедрялось в нашей стране с начала 1990-х годов, став к настоящему времени неотъемлемым атрибутом любых предприятий.

Учитывая важную роль компьютерных приложений в повышении эффективности налоговой и бухгалтерской деятельности всех предприятий страны, актуальность приобретает проблема дальнейшей оптимизации этих приложений. При этом, в интересах большинства предприятий, критериями оптимизации предлагается выбрать критерии эффективности: либо улучшение программ при неизменных затратах пользователей, либо снижение затрат пользователей при сохранении имеющихся функций программ, либо одновременное улучшение результата и снижение затрат (достигается инновациями, технологическим прогрессом).

Рассмотрение указанной проблемы логично начать с анализа динамики изменений бухгалтерских программ, существенных для большинства российских предприятий. В этой связи интерес представляют наиболее распространённые бухгалтерские программы и временной отрезок с начала 1990-х годов. Задачами такого анализа являются следующие. Во-первых, необходимо выявить наличие процесса постепенного непрерывного улучшения бухгалтерских программ, выражающегося в их оптимизации (критерии оптимизации приведены выше) для большинства пользователей-бухгалтеров и российских предприятий в целом. Такой процесс определяется нами как эволюция бухгалтерских программ. Во-вторых, необходимо определить факторы, сдерживающие эволюцию бухгалтерских программ. В-третьих, целесообразно разработать рекомендации субъектам государственного регулирования по ускорению эволюции бухгалтерских программ.

Анализ статистики и мнений экспертов показывает, что бухгалтерские программы 1С применяются более чем 80% процентами российских пользователей-бухгалтеров.

Формально эволюция бухгалтерских программ 1С представляется производителем как последовательность сменяющих друг друга версий. Так программа «Предприятие» версии 7.7 (выпущена в 1999 году) сменяется версией 8.0 (2003 год), а затем следуют версии 8.1, 8.2 и 8.3.

Новые версии программ, возможно, принесли улучшения с точки зрения программистов и отдельных групп предприятий, составляющих меньшинство. Однако спорным остаётся вопрос о наличии таких улучшений, которые касаются большинства предприятий и которые при этом не могли бы быть реализованы в рамках частичных обновлений программы версии 7.7. Как правило, с внедрением новых версий старые версии со временем прекращают обновляться и теряют актуальность по мере изменения законодательства и операционных систем (таких как Windows). В любом случае, смена версий программ не может рассматриваться только как необходимое следствие прогресса, так как он имеет важный экономический смысл для производителя. Так переходу на новые версии обычно сопутствуют: организация платных курсов для многочисленных бухгалтеров и программистов, на которых разъясняются особенности работы на новых версиях программы; доходы производителя от продажи программ новой версии и от продажи услуг по их установке на рабочие места, настройке и конфигурированию под особенности предприятия.

В этой связи задачи государственного регулирования бухгалтерских программ на настоящем этапе лежат, по нашему мнению, в сфере предотвращения возможных злоупотреблений предпринимателями своим монополистическим положением.

Дзюбенко И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

МОДЕЛЬ ОЦЕНКИ ВРЕМЕННЫХ ХАРАКТЕРИСТИК ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СЕТИ IoT

Одним из активно развивающихся направлений информационных технологий является Интернет вещей (Internet of things – IoT). IoT – совокупность разнообразных приборов, датчиков, устройств, объединённых в сеть посредством доступных каналов связи, использующих:

- ZigBee, Wi-Fi, Bluetooth и другие протоколы беспроводной связи малой зоны действия для взаимодействия между собой;
- IP-протокол для доступа в Интернет.

Примером IoT является сеть «умного дома». Несколько таких «умных сетей» могут быть объединены в сеть мониторинга и управления системой пожаротушения города, а «умные городские сети» в свою очередь могут быть объединены сетью Интернет для общего доступа к информации об уровне пожарной безопасности на любой территории страны.

Технология IoT находится на стадии ранней реализации и активных исследований. В частности актуальными вопросами являются оптимальная организация сети IoT с учётом требований к ее быстродействию, формату данных, энергосбережению узлов IoT.

С учетом этих требований среди различных методов физической организации IoT предпочтение отдаётся методу централизованного сервера, поскольку нагрузка, связанная с обработкой данных переносится на сервер, кроме того предоставляются надёжные средства хранения и обработки, в том числе облачные вычисления.

Передача данных от датчика, прибора или устройства (интернет вещи - ИВ) на сервер является стохастическим процессом, и в общем случае состоит из следующих этапов:

- накопление информации; включение или выход из режима сна ИВ;
- установка соединения с сервером; передача информации на сервер;
- переход в спящий режим или выключение ИВ.

Многоэтапность процесса передачи данных в IoT позволяет оценивать его временные характеристики, прибегая к методу декомпозиции.

В работе предлагаются следующие модели:

- установления соединения с сервером;
- преобразования форматов пакетов данных территориально распределенной сети интернета вещей;
- оценка времени передачи с учетом мультидоступа к серверу.

Корзина М.И., Антонов М.И., Корзин Ю.Н.
Россия, г. Архангельск, Северный (Арктический) федеральный университет имени М.В. Ломоносова, АТП «Панорама Retail»

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДИАГНОСТИКИ КОНТРОЛЬНО-КАССОВОЙ ТЕХНИКИ

Обслуживание контрольно-кассовых машин требует подготовки кадров и больших знаний в данной области. С каждым днем количество техники становится все больше и больше, как новых моделей, так и модификаций уже имеющихся. У каждой модели есть свой набор ошибок, инструкции и правил по эксплуатации, а, следовательно, с ростом количества техники растет и количество этих данных. Поэтому наличие информационной системы диагностики контрольно-кассовых машин значительно бы упростило работу с ними.

В результате анализа предметной области выявлено, что такая информационная система должна иметь следующие возможности: использования ИС без установки и наличия каких-либо дополнительных программных продуктов и библиотек; разграничения прав пользователей информационной системы; получения перечня ошибок по заданному номеру модели ККТ; поиска решения устранения ошибки по заданному коду ошибки; нахождения альтернативного решения по устранению ошибки; просмотра рейтинга решения по заданной проблеме в работе ККТ; группировки определенных моделей ККТ; редактирования перечня ошибок определенной ККТ; редактирования решения по устранению ошибки; получения сведений о выбранной ККТ; добавления новой контрольно-кассовой техники и сведений о ней; создания текстового отчета; вывода результата запроса; поиска необходимой информации; синхронизации базы данных между разными версиями информационной системы; воспользоваться подсказкой по использованию информационной системы специалисту.

В процессе проектирования системы были рассмотрены следующие аналоги: ALV Brain 1.31, Typer 1.23 SE, Expert Developer Pro МЭС 2.0 и др. Но данные программные продукты имеют ряд недостатков, например, отсутствие возможности создания текстового отчета, вывода результата запроса, иерархии каталогов данных и др.

Определены требования к информационной системе (ИС). ИС должна быть портативной и запускаться на любом устройстве под ОС Windows. В ИС должна присутствовать авторизация с разграничением прав пользователей, например, для возможности или ее отсутствия добавления и редактирования данных. Должна быть возможность добавления и редактирования данных внутри информационной системы без перекомпиляции системы. Данные должны быть представлены в виде иерархии каталогов с возможностью их сортировки и поиска по заданным критериям.

В качестве реализации БД на этапе физического моделирования было выбрано решение в качестве СУБД “MySQL”, язык программирования “PHP”, “JavaScript” для элементов управления ИС, взаимодействие между “JavaScript” и “PHP” будет осуществляться при помощи “Ajax”, оболочкой для реализации БД был выбран программный продукт “cPanel”, а клиент-серверного приложения – “Notepad++”.

Проведено тестирование на следующих устройствах: ноутбук с ОС “Windows 7 Home Premium x64” в браузере “Opera 37”; планшетное устройство на ОС “Android 4.4.2” в браузере «Chrome»; мобильный телефон на ОС “Windows 8.1”; мобильный телефон на ОС “iOS 7”. На всех устройствах информационная система работает корректно.

Рабочая ИС удобна и проста в использовании с наличием справки при возникновении вопросов по ее работе. ИС работает на любой ЭВМ типа ПК или мобильного устройства независимо от архитектуры ЭВМ и ОС.

Сальникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ КУЛЬТУРНОЙ ПОЛИТИКИ ЧЕРЕЗ РАЗВИТИЕ ТРАНСЛЯЦИЙ В КИНОТЕТАРАХ

В 2014 году, объявленном на территории Российской Федерации Годом культуры, была принята серия законодательных актов, среди которых «Основы государственной культурной политики». Целями государственной культурной политики является создание условий для воспитания граждан, сохранение исторического и культурного наследия и его использование для воспитания и образования, а также обеспечение доступа граждан к знаниям, информации, культурным ценностям и благам. Предприятия кинопоказа являются неотъемлемым компонентом сферы услуг, обеспечивая формирование ценностных ориентаций у населения и развитие культурного общественного потенциала. Такие предприятия - это посредник между производителями и потребителями услуг киноиндустрии. В связи с этим одним из перспективных направлений развития кинобизнеса является реализация на базе кинотетаров различных социально-культурных и образовательных программ в целях решения задач государственной культурной политики, а именно:

- поддержка профессиональной творческой деятельности в процессе создания и представления обществу произведений литературы, музыки, изобразительного искусства, драматургии, киноискусства, архитектуры, дизайна, художественной фотографии, иных видов искусства.
- развитие инфраструктуры культурной деятельности, создания благоприятной культурной среды в малых городах и сельских поселениях, включая создание клубной сети киновидеопоказа;
- восстановление и развитие системы воспитания и самовоспитания взрослых граждан;
- вовлечение в процесс воспитания граждан всех возрастов общественных организаций, научного и культурного сообществ, организаций культуры;
- развитие культурного просветительства с привлечением к этой деятельности профессиональных сообществ и организаций культуры.

Одна из задач государственной культурной политики в области осуществления всех видов культурной деятельности и развития связанных с ними индустрий определена как «государственная поддержка отечественной кинематографии, в том числе создания анимационных, документальных, научно-популярных, учебных, адресованных детской аудитории фильмов, создание условий для развития творческих индустрии». Также в Основах культурной политики указано, что «творческие индустрии» – это компании, организации и объединения, производящие экономические ценности в процессе творческой деятельности, а также деятельность по капитализации культурных продуктов и их представлению на рынке. Из данных определений следует, что при государственной поддержке деятельности по социально-культурному обслуживанию населения каждое предприятие кинопоказа является творческой индустрией, развитие которой должно соответствовать целям и стратегическим задачам государственной культурной политики, ключевым принципам ее реализации.

Богатое историческое и культурное наследие и возможности современных информационных технологий создают неограниченное пространство для составления программ кинопоказа. Организация кинопоказов предполагает не только просмотр различных фильмов (текущий кинопрокат, художественные фильмы разных времен, документальные записи и т.д.), но и новых видов визуальных продуктов. Например, кинотеатры могут предлагать к показу виртуальные экскурсии по музеям, по городам и другим культурным и природным достопримечательностям России и всего мира, а также трансляции различных культурных мероприятий.

В настоящее время успешно реализованы проекты «Большой балет в кино» и «Театральная Россия», в рамках которых спектакли Большого театра и различных драматических театров стали доступны зрителям самых разных городов и стран. В настоящее время в прямых трансляциях и повторных показах участвуют более тысячи кинотеатров в пятидесяти странах мира, включая города России (свыше тридцати городов и сорока кинотеатров).

Очевидно, что данная практика показа культурных событий в прямой трансляции и в записи имеет огромный потенциал для развития всех кинотеатров в России, особенно на территориях, удаленных от больших городов и мегаполисов.

Развитие системы культурных трансляций в предприятиях кинопоказа должно являться задачей государственного значения и поддерживаться соответствующими законодательными актами, что

позволит реализовать одну из задач государственной культурной политики в области осуществления всех видов культурной деятельности и развития связанных с ними индустрий - сохранение и развитие единого культурного пространства России, в том числе путем использования цифровых коммуникационных технологий для обеспечения доступа граждан к культурным ценностям независимо от места проживания. А понимание, что в современном мире культура является значимым ресурсом социально-экономического развития, позволит обеспечить конкурентоспособное положение предприятиям кинопоказа на российском рынке киноиндустрии.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Бачиев Р.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ЗАДАЧА РАСПОЗНАВАНИЯ СЛОЖНЫХ СИТУАЦИЙ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

В настоящее время обработка цифровых изображений с целью распознавания ситуаций является сложной задачей. Эта задача может решаться на различных объектах (метро, площади, торговые и развлекательные центры, критически важные предприятия и другие), на которых поддержание порядка и недопущение чрезвычайных ситуаций является приоритетной целью. Для ее решения требуется наличие соответствующих методов. Анализ известных методов показывает, что они во многом не совершенны.

В большинстве случаев для распознавания ситуаций в настоящее время применяются методы обработки динамических изображений, основанные на детектировании объектов по особым точкам, выделении признаков движения объектов на основании нескольких изображений или кадров видео одной и той же сцены. Однако недостатком такого подхода является узкий круг решаемых задач. В частности, такие методы способны только следить за траекторией движения объектов, детектировать их столкновения, удары, переходы в запрещенные зоны и т.д.

Так же для обработки видеопотока используются методы, основанные на обработке обучающих выборок (статистический, графовый, метод k ближайших соседей и другие). Однако они требуют большого объема обучающих выборок и используются вместе с другими методами. Имеют место и другие недостатки этих методов. Также общим недостатком таких методов является чувствительность к шумам во входных данных.

Одним из перспективных подходов выступает использование биологических принципов, в частности использование нейросетевых методов обработки информации. Такие методы уже показали свою высокую эффективность в задачах классификации и прогнозирования. Нейронные сети обладают рядом важных качеств, которые будут способствовать качественному решению задач. Среди них можно выделить адаптивность и низкую восприимчивость к шумам в исходных данных. Одним из лучших алгоритмов распознавания и классификации изображений является сверточная нейронная сеть. Ее преимуществом сравнительно с другими нейронными сетями является гораздо меньшее количество настраиваемых весов, удобное распараллеливание вычислений, возможность обучения с помощью метода обратного распространения ошибки. Однако эти сети не в полной мере ориентированы на обработку видеопотоков. Необходим поиск более совершенных подходов для решения этой задачи.

Предлагается исследовать возможности обработки видеопотоков в реальном времени с применением развиваемых рекуррентных нейронных сетей с управляемыми синапсами.

Михайленко Е.И., Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»

РАЗВИТИЕ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Системы критических инфраструктур, в соответствии с предъявляемыми к ним требованиями, должны осуществлять безопасный информационный обмен с использованием ресурсов телекоммуникационных сетей связи. Телекоммуникационные сети связи общего пользования является составной частью единого информационного пространства общей автоматизированной системы управления и базируется на элементах специальных систем связи, а также на транспортных ресурсах, арендованных у операторов связи единой системы электросвязи (ЕСЭ) России.

В настоящее время актуальными направлениями развития телекоммуникационных сетей связи являются:

- цифровизация транспортной сети связи и сетей доступа, создание интегрированной цифровой транспортной сети на основе волоконно-оптических SDH/WDM/DWDM и VSAT-технологий;
- расширение номенклатуры предоставляемых услуг и повышение их качества;
- интеграция служб и услуг на основе создания широкополосных сетей связи с интеграцией служб с применением технологий MPLS;
- создание интеллектуальных сетей и сетей связи следующего поколения (NGN).

В целом данные направления развития свидетельствуют о поэтапном переходе от построения узкоспециализированных выделенных сетей связи к цифровым перспективным сетям связи (ПСС) с

пакетной коммутацией. В общем случае построение ПСС за счёт унификации сетевых решений обеспечивает:

– предоставление и интеграцию широкого спектра услуг с требуемым качеством обслуживания;

– гибкость и адаптацию к изменению уровня требований пользователей к объёму, скорости и качеству доставки информации, а также к появлению требований на предоставление новых видов услуг;

– минимизацию затрат на развитие и эксплуатацию сети.

Вместе с тем построение ПСС требует новых подходов к вопросам обеспечения качества обслуживания при совместной передаче трафика различных служб, особенно в условиях ограниченных сетевых ресурсов и обеспечения безопасности информации.

АСУ территориально распределенными объектами имеют ряд общих особенностей, которые позволяют выделить для исследования объект – АСУ критических инфраструктур (АСУ КИ), и на его базе провести обоснованный анализ и синтез ее телекоммуникационной сети. Как правило, в АСУ КИ значительная часть элементов управления (ЭУ) являются подвижными объектами (ПО). Необходимость обеспечения высокой динамики управления различными ПО в современных изменяющихся условиях требует совершенствования как АСУ КИ в целом, так и ее сети связи, являющейся технической основой управления.

Актуальным и приоритетным направлением развития элементов АСУ КИ становится всесторонняя интеграция и повышение уровня взаимодействия на основе создаваемого единого информационно-разведывательного пространства (ЕИРП) и единого информационно-управляющего пространства (ЕИУП) элементов управления за счет реализации сетеориентированного подхода и bнтеграции оружия и его носителей, систем управления, связи и навигации, средств разведки и обеспечения на любом театре военных действий. Системообразующим элементом сетеориентированного подхода являются телекоммуникационные сети (ТКС).

Однако сегодня имеется ряд проблемных вопросов в направлении создания ТКС и систем, действующих на принципах сетецентрического управления (СЦУ). Это, прежде всего, реализация сильносвязного пространства с многочисленными взаимоувязанными средствами сете- и каналообразования, выстроенного по принципам их иерархий с сильно развитыми вертикальными и горизонтальными межвидовыми связями ЕИРП КИ.

Для реализации принципов СЦУ необходима широкополосная высокоскоростная транспортная сеть, при этом широкополосная связность пространства должна доходить до мобильного высокоскоростного объекта. Главным принципом этой структуры становится обеспечение постоянной связи между любыми потребителями, в любое время, в любом месте, в любой обстановке.

При этом современные инфокоммуникационные технологии работают на фундаменте, заложенном полвека назад.

Перспективная телекоммуникационная среда должна строиться как сеть с коммутацией пакетов на базе перспективного стека протоколов, используя технологию, получившую название программно-определяемых сетей и виртуализации сетевых функций (SDN и NFV). В общем случае SDN/NFV – это сеть передачи данных, в которой уровень управления отделён от сетевых устройств передачи данных и реализуется программно на базе стандартных аппаратных платформ.

Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»

ГИБРИДНЫЙ ПРОТОКОЛ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Рассмотрим беспроводную сеть, которая состоит из нескольких ad hoc компонентов (Mobile Ad Hoc NETworks – сети без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией) и стационарных маршрутизаторов области ретрансляторов, которые работают в качестве ядра сети. Каждый ad hoc компонент рассматривается как отдельный регион. Маршрутизатор, подключенный к этому региону, несет ответственность за выдачу адресов узлам, маршруты к узлам других регионов и сетей и управление в этом регионе. Предлагаемый протокол маршрутизации состоит из трех компонентов маршрутизации:

– протокола маршрутизации внутри ad hoc региона (Intra Region Routing Protocol) – IRRP;

– протокола маршрутизации стационарных маршрутизаторов области ретрансляторов (Router Infrastructure Routing Protocol) – RIRP;

– протокола маршрутизации между ad hoc регионами (Region Gateway Routing Protocol) – RGP.

Маршрутизаторы области ретрансляторов используют Router Infrastructure Routing Protocol. Поскольку маршрутизаторы области ретрансляторов статические, RIRP относится к семейству беспроводных активных протоколов маршрутизации. RIRP работает на каждом статическом маршрутизаторе и обеспечивает маршруты в регионы, связанные с маршрутизаторами. Таблицы

маршрутизации всегда актуальны, чтобы обеспечить немедленную маршрутизацию. Это позволяет существенно сократить задержки при определении маршрута.

В конкретном регионе или ad hoc компоненте маршруты поддерживаются с помощью протокола Intra Region Routing Protocol (IRRP). IRRP – это реактивный протокол маршрутизации, который поддерживают расширенный поиск маршрутов и услуги технического обслуживания маршрута на основе локальных подключений к региону в режиме ad hoc.

Region Gateway Protocol используется, когда требуется маршрут между двумя ad hoc узлами разных регионов. Он получает информацию о маршрутах от RIRP и IRRP и создает полный маршрут от источника к получателю и предоставляет его в исходный узел. Когда узел требует маршрут, RGP получает информацию от RIRP и IRRP обоих ad hoc регионов, строит маршрут и отправляет его IRRP и RIRP.

Всякий раз, когда новый маршрутизатор включается в сеть или в случае сбоя соединения, RIRP должен знать о событии. Для этого RIRP использует либо Neighborhood Discovery Protocol (NHDP) для доступа к MAC-уровню или обеспечивает эти функциональные возможности самостоятельно. Каждый узел посылает hello-пакеты, содержащие информацию о соседних узлах, другим узлам в этом районе через постоянные интервалы времени. Если время ожидания истекает и hello-пакет не получен, то можно сказать, что есть проблема с соединением. Благодаря такому обмену каждый узел сети получает представление об узлах в двухшаговой окрестности и о свойствах соединений между этими узлами.

Аналогичным образом, когда новый узел приходит в сеть, он может заявить о себе, передавая hello-пакет.

Всякий раз, когда узел должен послать некоторые данные другим узлам, он проверяет, имеет ли он маршрут к месту назначения. Если активного маршрута нет, узел начинает фазу обнаружения маршрута. Механизм обнаружения маршрута имеет три этапа: запрос маршрута, формирование маршрута и маршрут-ответ.

На этапе запроса маршрута запрос посылается в соседние узлы, используя IRRP. Если соседние узлы не имеют маршрута до места назначения, они пересылают запрос другим узлам. Если ни один узел не имеет маршрут до пункта назначения, запрос отправляется на RGP, работающий на маршрутизаторе, подключенном к ad hoc компоненту. Здесь RGP пытается найти маршрутизатор, подключенный к необходимому ad hoc компоненту с помощью RIRP. Когда маршрут к маршрутизируемому узлу найден, RGP использует IRRP в ad hoc регионе, в котором находится узел назначения, чтобы найти к нему путь.

После того, как маршрут до пункта назначения находится, весь маршрут от источника до пункта назначения формируется посредством RGP. Эта фаза называется фазой формирования пути. Когда полный маршрут сформирован, маршрут-ответ с полной информацией отправляется к исходному узлу, на этом фаза поиска маршрута завершается.

Для активного компонента предлагается использование протоколов Destination Sequenced Distance Vector (DSDV) или Optimized Link State Routing (OLSR). Эти протоколы маршрутизации имеют процедуры поиска маршрута в области инфраструктуры стационарных маршрутизаторов. Кроме того, для выполнения этой задачи в ad hoc регионах предлагается использовать протокол Adhoc Ondemand Distance Vector (AODV) в качестве реактивного протокола маршрутизации. Необходимо разработать реализацию Region Gateway Protocol, который вычисляет весь маршрут и предоставляет его запрашивающему узлу.

Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»

МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ СЕТЯХ

В беспроводных сетях могут быть мобильны не только рабочие станции, но и сами маршрутизаторы. В таком случае узел состоит из маршрутизатора и хоста одновременно, они даже могут быть совмещены в пределах одного устройства. Кроме того, топология таких сетей постоянно меняется, а с ней меняется и предпочтительность (и даже реализуемость) путей.

Такие сети являются подклассом беспроводных сетей, это так называемые сети MANET (Mobile Ad Hoc NETworks) – сети без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией. Каждый узел в мобильной ad hoc сети работает одновременно подобно конечной системе и маршрутизатору.

Особенности беспроводных сетей приводят к тому, что протоколы и технические решения, используемые в классических проводных сетях, например централизованная маршрутизация с иерархией заранее назначенных маршрутизаторов, в мобильных сетях без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией оказываются неэффективными и не обеспечивают нужную производительность.

Одной из ключевых задач в многошаговых беспроводных сетях является задача поиска маршрута между двумя станциями (задача маршрутизации). Протоколы маршрутизации, работая на

сетевом уровне, не взаимодействуют с канальным уровнем. Таким образом, им недоступна информация о вероятности искажения пакетов помехами и коллизиями, о свойствах сигнально-кодовых конструкций, о методе доступа к каналу и параметрах механизма повтора непринятых пакетов. Следовательно, эти протоколы не могут определить вероятность успешной передачи пакета по соединению, а также пропускную способность соединения, а маршруты, найденные с их помощью, обладают малой пропускной способностью и часто пропадают. Кроме того, протоколы маршрутизации зачастую не учитывают особенности беспроводной среды.

Для повышения эффективности протоколов маршрутизации в беспроводных сетях их необходимо снабдить информацией о канальном уровне, например, о качестве соединений с помощью метрики маршрутизации. Другой подход заключается в решении задачи маршрутизации на канальном уровне.

При разработке большинства алгоритмов оптимизации основное внимание уделялось вопросам взаимодействия распределенных узлов для формирования маршрута, при этом использовались простейшие критерии оценки оптимальности полученного маршрута. В большинстве протоколов таким критерием является длина маршрута, т.е. число узлов задействованных при передаче информации. В отдельных случаях также учитывалась максимальная пропускная способность связей между двумя узами. В идеальном случае оценка оптимальности на основе данных параметров позволяет выбрать наилучший маршрут, однако не учитывает ряд параметров, которые присутствуют в сетях при практическом применении. Для беспроводных сетей такими параметрами могут быть учет уровня сигнала для канала между двумя узлами и параметры текущей загрузки отдельных фрагментов маршрута.

По принципу поиска маршрута выделяют три класса протоколов: проактивные, реактивные и комбинированные.

И проактивные, и реактивные протоколы маршрутизации имеют свои преимущества и недостатки, которые делают их пригодными для определенных условий функционирования сети. Так как протоколы проактивной маршрутизации обрабатывают информацию так, что она сразу же доступна, задержка перед отправкой пакета является минимальной. Напротив, протоколам реактивной маршрутизации необходимо сначала определить маршрут, что может привести к значительной задержке, если информация не доступна в кэше.

Кроме того, реактивная процедура поиска маршрута требует значительного контроля трафика из-за лавинного распространения служебных пакетов. Это вместе с большой задержкой определения маршрута может сделать реактивную маршрутизацию менее пригодной для трафика, критичного к времени.

Тем не менее, объем трафика может быть уменьшен за счет использования схемы обслуживания маршрута. Чисто активные схемы используют большую часть пропускной способности для поддержания актуальности маршрутной информации. Вследствие быстрой мобильности узлов обновления маршрутов могут быть более частыми, чем запросы маршрутизации, и большая часть информации о маршрутизации никогда не используется. Некоторая часть из дефицитной пропускной способности, таким образом, тратится впустую.

Лучшим решением было бы использовать различные протоколы маршрутизации для различных частей сети. Реактивный протокол можно использовать для контроля динамического изменения топологии и подвижности узлов. Активный протокол лучше подошел бы для статических узлов, чтобы обеспечить быструю доступность маршрутов.

Путилин А.Н., Шаптала В.С.
Россия, Санкт-Петербург, АО«НПО «Импульс»

АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ МАЛАГАБАРИТНОЙ СТАНЦИИ ТРОПОСФЕРНОЙ РАДИОСВЯЗИ

Станции тропосферной радиосвязи (ТРС) «Сосник-4П» производства АО «НПП «Радиосвязь», г. Красноярск и «Ладья» производства МНИИРС, г. Москва являются весьма востребованными для решения ряда задач по организации высокоскоростной связи в труднодоступных районах. При низком энергопотреблении, габаритах и стоимости они устойчиво работают на скоростях передачи от 64 до 512 кБ/с.

Предлагаются реализация следующих технических решений по их совершенствованию:

1. Параллельный OFDM модем, который позволит в два раза увеличить техническую скорость передачи при сохранении полосы сигнала 4 МГц.
2. Алгоритм синхронизации по рабочей посылке, не требующий передачи синхропреамбул.
3. Алгоритм «слепой» частотной адаптации, состоящего в переходе на следующую по номеру частоту при браковке рабочей частоты. В отличие от прототипа он не требует тестирования всех частот, позволяет работать с пакетом частот любой ёмкости без модификации алгоритма.

4. Алгоритм регулировки скоростей обмена в прямом и обратном направлении связи при реализации режима псевдо дуплекса, который обеспечит реализацию ассиметричного канала передачи данных для эффективной работы систем повышения достоверности с обратной связью.

Аналитическое и имитационное моделирование функционирования линии ТРС при реализации в ней предложенных технических решений показало, что без изменения условий функционирования, энергетики и полосы сигнала обеспечивается достижение скоростей передачи от 230 Кб/с до 3,4 Мб/с. Произведён расчет вычислительной сложности для алгоритмов модуляции/демодуляции для частоты дискретизации: 8,192 МГц. Установлена возможность реализации этих алгоритмов модуляции и демодуляции на недорогом многоядерном процессоре архитектуры x86.

Предложенная модификация алгоритмов функционирования малогабаритной станции ТРС позволит в любом районе радиусом от 100 до 300 км обеспечить группировку сил и средств МЧС, МО, МВД и других министерств и ведомств надёжной высокоскоростной связью. Необходимое оборудование будет иметь минимальные массогабаритные характеристики.

Стародубцев Ю.И., Чеснаков М.Н., Латушко Н.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

УПРАВЛЕНИЕ ПРОЦЕССАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Критическая информационная инфраструктура Российской Федерации (далее - критическая информационная инфраструктура) - совокупность автоматизированных систем управления критически важных объектов (далее КВО) и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий.

Использование сетей связи общего пользования для информационного обмена системами управления, производственными и технологическими процессами КВО, глобализацией современных информационно-телекоммуникационных сетей, превращением их в единую мировую информационно-телекоммуникационную сеть с размытыми границами национальных сегментов, делает затруднительным обеспечение безопасности автоматизированных систем управления КВО, без обеспечения безопасности Единой сети электросвязи Российской Федерации в целом.

Большинство протоколов, в соответствии с которыми функционируют сети, разрабатывались без учета необходимости защиты от действий злоумышленников. В протоколах маршрутизации практически отсутствуют механизмы защиты от атак, которые изменяют, удаляют, подменяют или воспроизводят перехваченные данные и могут вносить существенные помехи в работу системы маршрутизации. Темпы возникновения новых угроз, использующих уязвимости сетевых протоколов, значительно превышают темпы совершенствования предусмотренных в них механизмов защиты.

Злоумышленники, имея доступ хотя бы к одному узлу сети, могут внести существенные искажения в работу сети путем навязывания ложной маршрутной информации. Существуют также некоторые методы нарушения работы сети в целом путем разрыва связей в системе обмена информацией между узлами. Криптографическая аутентификация обмена данными между узлами используется не всегда. Внешние источники обманной информации могут располагаться в любой точке сети Internet.

Типы воздействий на сеть, оказываемые злоумышленниками с целью нарушения работы критической информационной инфраструктуры:

- Трафик, адресованный узлу, пересылается в ту часть сети, которая не может обеспечить его доставку;
- Через часть сети в некоторые моменты времени может пересылаться больше данных, чем эта сеть способна обработать;
- Большое количество трафика направляется для пересылки через маршрутизатор, который не способен справиться с возросшим уровнем трафика, что приведёт к потере части или всех IP-пакетов;
- Данные, адресованные узлу, пересылаются не по кратчайшему пути, с целью увеличить время доставки;
- Данные передаются по замкнутому пути и никогда не будут доставлены;
- Данные пересылаются через какой-либо маршрутизатор или сеть, которые не должны видеть эти данные, информация при такой пересылке трафик может просматриваться;
- Части сети могут казаться отрезанными от сети, хотя реально они подключены;
- Скорость пересылки в сеть начинает изменяется быстрыми темпами, что приводит к значительным вариациям картины доставки пакетов;
- Работа протоколов маршрутизации становится нестабильной и не удается достичь схождения картины маршрутов;

– Маршрутная информация становятся значительной частью передаваемого через сеть трафика;

– Данные пересылаются через некий маршрутизатор или сеть, которые являются подставными и могут служить для перехвата или искажения информации.

Уязвимость ЕСЭ РФ перед большим числом различных деструктивных воздействий, ставит задачу разработки способов сокрытия факта функционирования критической информационной инфраструктуры Российской Федерации на том или ином фрагменте сети связи общего пользования, эта задача не может решаться однозначно и статично, в этой связи, возникает задача разработки алгоритмов оптимального управления.

Федосеев С.С.
Россия, Санкт-Петербург, АО «НПО «Импульс»

ОЦЕНКА ЭНЕРГЕТИЧЕСКИХ ХАРАКТЕРИСТИК РАДИОКАНАЛОВ ПУТЕМ СТАТИСТИЧЕСКОГО АНАЛИЗА РЕЗУЛЬТАТОВ ДОВЕДЕНИЯ СООБЩЕНИЙ

Непосредственное определение энергетического запаса в радиоканалах известными методами не всегда возможно.

Так, например, для каналов, использующих радиосигналы с расширением спектра типа ШПС ФМ, уровень сигнала на приёмной стороне находится значительно ниже уровня естественных атмосферных шумов и недоступен для измерения.

Метод оценки энергетического запаса посредством определения качества канала по уровню ошибок в битовом потоке (Ро) требует априорной известности передаваемого сообщения, что в ряде практических применений не всегда возможно. Не всегда возможно также получить доступ к электрическим цепям радиоприёмной аппаратуры для анализа битового потока.

Метод с использованием серии испытаний радио тракта с последовательным ступенчатым уменьшением мощности на передающей стороне и контролем выполнения заданного критерия качества на приёмном конце можно отнести к методам непосредственного определения энергетического запаса в канале. Однако, применение данного метода ограничено в связи с его дороговизной. Кроме того, не всегда есть техническая возможность ступенчатого понижения мощности передатчика.

Предлагается методика определения энергетического запаса в радиоканале путём статистического анализа результатов испытаний доведения сообщений.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ

Александров В.В., Зайцева А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

РАЗРАБОТКА ПОДХОДОВ К ОПРЕДЕЛЕНИЮ КУЛЬТУРОЛОГИЧЕСКИХ КАНОНОВ РАЗЛИЧНЫХ СОЦИАЛЬНЫХ ГРУПП НА ОСНОВЕ МЕТОДОВ АНАЛИТИЧЕСКОГО САМОРЕФЕРИРОВАНИЯ

Проблема информационной безопасности сегодня все еще преподносится в большей степени как инженерно-техническая, структурно-организационная и технологическая дисциплина. Самые совершенные научные и технологические разработки касаются программ криптографии, стеганографии, защиты от несанкционированного пользования. Эта информационная защита не имеет ничего общего с защитой информационного общества от общественно опасных информационных потоков.

Потенциально опасные сведения легко найти на сайтах социальных сетей, микроблогов и сообществ Интернет. Прогресс электронных технологий получения и распространения информации вызывает потребность в создании технологии обеспечения безопасности информационного общества.

Рост количества доступных в Интернет ресурсов сопровождается появлением в свободном доступе материалов потенциально опасного содержания: призывы к незаконным действиям, пособия «начинающего террориста», изображения порнографического характера и другие нежелательные материалы.

Использование подходов с привлечением поисковых систем, основанных на использовании тематических и индексных каталогов, неэффективно по причине ограниченности области поиска при использовании только набора ключевых фраз. Поэтому необходимо разрабатывать комплексные решения, основанные на алгоритме информационного поиска, объединяющего семантический поиск в сетях (базах данных), поиск по нормативным документам и мониторинг информационных ресурсов.

Основная особенность предлагаемого подхода состоит в организации поиска ресурсов и сообщений, удовлетворяющих условию наличия семантических связей в тексте между всеми словами поискового запроса. Инфологический подход позволяет организовать разноуровневые глоссарии предметной области (возможность использования эксперта).

Одной из главных задач, решаемых разрабатываемым подходом, является построение кадастра предметной области для дальнейшего мониторинга с целью раннего обнаружения террористических угроз, выявления смены тональности высказываний в различных социальных группах, в зависимости от возраста, социального положения, местожительства и т.д.

Для этого к контенту, генерируемому пользователями в различных группах и сообществах социальных сетей, применяется разработанный в лаборатории автоматизации научных исследований метод автоматического самореферирования в сочетании с использованием инфологической системы мониторинга электронных СМИ.

Мониторинг электронных СМИ позволяет выявлять зависимости между людьми и событиями, а также круг актуальных, по версии общественного мнения, вопросов. Теоретически с увеличением объемов новостных текстов увеличивается точность их семантического анализа и повышается релевантность результатов поиска.

Методы аналитического самореферирования основаны на выявлении понятийного иерархического окружения слов текста и ассоциативно-понятийной трансляции исходного текста, при этом производится итеративная рейтинговая фильтрация – процесс сокращения объема реферируемого текста при сохранении семантики, который регулируется уровнем понятийной терминологической иерархии.

Таким образом, построение глоссариев культурологических канонов и деструктивных мемов предметно-тематических групп социальных сетей отличается использованием динамической визуализации онтологического окружения словаря предметной области. Далее применяются методы кластеризации на основе ранговых предпочтений и ассоциативно-категориального поиска в информационно-социальных сетях с целью оценки степени террористической угрозы.

Александров В.В., Кулешов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЦИФРОВАЯ ПРОГРАММИРУЕМАЯ ЭЛЕКТРОНИКА

Отставание России в цифровой электронике проистекает из середины XX-го века, знаменитой научной революцией: освоением космоса, атомной энергетикой, общей теорией информации, кибернетикой, персональными компьютерами и оптоэлектроникой. Революция в этих областях сопровождалась острой научной дискуссией, как отклик на лекцию известного английского писателя и ученого Чарлза Перси Сноу «Две культуры и научная революция», прочитанную им в мае 1959 года в Кембриджском университете. Главная мысль лекции Сноу, послужившей затем основой для переведенной на многие языки одноименной книги, сводилась к утверждению того, что между традиционной гуманитарной культурой и новой, так называемой, «научной культурой», производной от научно-технического прогресса XX века, с каждым годом растет катастрофический разрыв. В настоящем — это цифровые программируемые технологии, квантовая коммуникация, а также степенной закон развития (закон Мура) цифровой технологии. Скорость и память процессоров косвенно мультиплицируют развитие техногнозиса и социума. Закон Мура распространяется не только на процессоры. Он полностью определяет развитие всех современных устройств и функциональных приложений. Можно, с одной стороны, гипотетически предположить, что закон Мура имеет отношение только к цифровым процессам, однако стоило начаться конвергенции цифровых и традиционных наук, как этот закон начал достаточно динамично распространяться в аддитивных (3D) и других технологиях.

Наиболее промышленно-развитые страны (в первую очередь, США) начинают выходить из индустриальной стадии своего развития. Они вступают в эпоху, в которой главенствуют технологии и особенно электроника (отсюда неологизм «технотронный»).

Постиндустриальное общество становится «технотронным» обществом, которое сформировалось культурно, психологически, социально и экономически в результате воздействия технологии и электроники, особенно в области компьютеров, средств коммуникации и связи.

Усиливающееся участие каждого человека в мировых делах отражается и, несомненно, формируется за счет изменения характера того, что до сих пор считалось местными новостями. Вслед за газетами, телевидение стало расширять горизонты восприятия зрителя или читателя до той точки, где «местный» уже означает «национальный», а глобальные вопросы начинают привлекать внимание в беспрецедентных масштабах. Физическая и моральная устойчивость к «иностранным» событиям не может эффективно поддерживаться в тех обстоятельствах, когда одновременно растет как интеллектуальное осознание глобальной взаимозависимости, так и вторжение глобальных событий в дом посредством электроники. Как метко заметил М. Делягин, человек придумывает технологии для собственного удобства, и они немедленно перекраивают и ломают его под себя, превращая в свой элемент, — вечная история, вот уже минимум полтора века являющаяся азбучной истиной, сохраняет всю остроту и ужас новизны для каждого поколения, которое затрагивает. Те самые технологии, которые предельно упростили коммуникации (процесс этого упрощения получил ставшее уже пошлым название «глобализация»), сделали наиболее рентабельным из общедоступных видов бизнеса трансформацию человеческого сознания.

Современный технологический уклад вызывает намного более глубокие перемены в жизни общества, чем распространение паровой машины, двигателя внутреннего сгорания, электричества, химических технологий и даже появление первого персонального компьютера.

Обучаться можно будет при помощи базовых мобильных услуг вроде текстовых месенджеров и медиаресурсов.

Появится возможность провести медицинский осмотр «изнутри» с помощью специальных устройств Использование таких устройств перестанет вызывать споры, как это случилось с кардиостимуляторами Они станут логическим продолжением современных приложений для контроля за персональным здоровьем.

После того как основные общественные институты: системы здравоохранения, образования и судебная система окончательно вступят в цифровую эру, они станут более эффективными, прозрачными и доступными.

Боруля П.Т, Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина)
РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АСУТП КРИТИЧНЫХ ИНФРАСТРУКТУР

Современное развитие промышленности подошло к четвертому этапу индустриальной революции, характерной особенностью которого является насущная необходимость интеграции науки и промышленности на основе развитых информационных технологий.

Усиленная интеграция «киберфизических систем» в производственные процессы приводит к возможности не только объединения станков в единую сборочную линию, но взаимодействия их друг с другом без участия человека. Идентификация выпускаемых изделий с использованием штрих-кодов, без участия человека, позволяет построить самоорганизованную производственную линию с отсутствием централизованного управления. Управление производственными процессами с использованием скоростной высокопроизводительной связи через мобильные устройства и Интернет позволяет применять новые бизнес-модели, такие как «совместное пользование» и «по заказу». Внедрение технологий промышленного Интернета связано с серьезной проблемой информационной безопасности: построение безопасных сетей является нетривиальной задачей, а интеграция физических систем, в виде оконечного промышленного оборудования, с Интернетом - делает их еще более уязвимыми к кибератакам. По мере развития Индустрии 4.0 наличие угроз дистанционного проникновения в указанные системы растет пропорционально квадрату числа сетевых узлов. Среди внешних атак на ресурсы промышленности наиболее распространенными остаются промышленный шпионаж, нарушение функционирования вредоносным кодом, случайные взломы. Особую опасность представляют нарушения функционирования процессов, контролируемых системой управления, при которых борьба с последствиями практически не будет отличаться от борьбы с техногенной аварией.

Применяемое в настоящее время программное обеспечение не позволяет осуществлять территориально-распределенное управления через сеть Интернет. В качестве наиболее характерных особенностей использования нарушений безопасности можно привести следующие:

- эксплуатация уязвимостей программного обеспечения Интернет вещей, при которых возможно отображение контента легитимного пользователя на стороне нарушителя («rickrolling»). Эксплуатация уязвимостей протоколов передачи, которые «наследуются» из стека протокола TCP/IP и протоколов стандарта IEEE 802.11;
- использование межмашинного взаимодействия, позволяющего осуществить компрометацию сервера, с которого осуществляется администрирование всеми устройствами, с возможностью дальнейшего управления со стороны нарушителя;
- отдельную опасность представляет угроза внедрения вирусов модульного типа.

Указанные тенденции демонстрируют, что время реакции и адаптации АСУТП на перемены, которые вызваны существующими угрозами безопасности, значительно превышают интервал между очередными изменениями, вносимыми для обеспечения безопасности. Это приводит к необходимости организации защиты критически важных объектов инфраструктуры, обеспечивающих гарантированное управление во всех требуемых условиях эксплуатации при случайных, техногенных и навязываемых дестабилизирующих факторах.

Это требует внедрения на предприятии новых информационных подходов, основанных на прогнозировании возможных проблем и разработки методических и методологических основ построения самоорганизующихся средств защиты информации. Возникает необходимость применения унифицированного интерфейса между подсистемами и базовыми модулями, с возможностью внешнего дополнения и детализации типовых компонент, обеспечивающих выбор необходимых и достаточных средств для управления. Это обеспечит единство подходов к управлению процессами обеспечения безопасности, в том числе обоснование принятия решения на основе применения модельных описаний объектов угроз безопасности, сценариев, принудительных мер обеспечения безопасности. Это позволит осуществлять пространственно- временную адаптацию к изменяющимся условиям внешней среды, путем переконфигурирования внутренних показателей структур мониторинга и оценивания текущего состояния инфраструктуры АСУТП и предложения по реализации их на практике. Такой подход позволяет осуществить два варианта построения системы управления безопасностью:

- Централизованный вариант, при котором центральный модуль управления осуществляет мониторинг за состояние всей инфраструктуры и обладает всей полнотой информации.
- Децентрализованный вариант, при котором каждое устройство осуществляет мониторинг и/или прогнозирование безопасности, затрачивая собственные ресурсы для обработки полученной информации. Указанные технологии являются масштабируемыми и обеспечивают оперативную реакцию на изменение условий внешней среды.

Бурлов В.Г. Мокеева Т.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

КОНЦЕПЦИЯ ПОДДЕРЖАНИЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ НА ОСНОВЕ ОБРАТНОЙ СВЯЗИ

Одной из сложных задач в организации производства является формирование функций управления. Основа управления производством – это решение руководителя. Сложность любого процесса управления заключаются в несоответствии полученных результатов требуемым, что обосновано противоречивыми выводами. Для исключения противоречивых выводов используется аксиоматический метод.

Аксиоматический метод предполагает существование следующих элементов:

- основные допущения и предположения, обычно выражающиеся в базовых принципах;
- базовые понятия, ключевые слова, аксиомы, правила вывода, теоремы;
- базовые принципы должны характеризовать суть процесса, с которым работает исследователь.

При этом в процессе деятельности участвуют три компонента: человек (его сознание), окружающий мир (объект), всеобщая связь. Человек принимает решение оперируя с категорией «процесс», на основе категория «модель», с позиции рассмотрения, как любого «объекта», так и «процесса» в целом, – в виде «системы».

В настоящий момент используются схемы решения задач управления на основе анализного подхода, т.е. запущенный процесс со входом и выходом. В такой схеме весьма проблематично учитывать возмущения. Если не учитывать возмущения, влияющие на процесс, то такой процесс с течением времени разрушается, и как следствие – не достигается цель производства. Во избежание такого развития событий, сформирована концепция поддержания функционирования системы управления на основе обратной связи. В основу обеспечения обратной связи положен закон сохранения целостности, а реализует обратную связь руководитель своим управленческим решением.

Закон сохранения целостности - это объективная устойчивая повторяющаяся связь свойств объекта и свойств его действия, проявляющаяся во взаимной трансформации свойств объекта и свойств его действия при фиксированном предназначении.

Процесс управления производством действует на основе закона сохранения целостности, и для того, чтобы этот процесс существовал, необходимо и достаточно установить связь между категориями «объект», «действие», «предназначение». С другой стороны применяя принцип познаваемости, мы должны расчленить процесс управления производством на эти три базовых элемента.

Далее мы должны интерпретировать «объект», как элемент модели «решения», в виде «обстановки». Это следует из того, в процессе формирования решения для лица принимающего решение не зависит только от «обстановки» (факторы и условия, в которых осуществляется деятельность).

«Действие» мы должны интерпретировать, как элемент модели «решения», в виде «информационно-аналитической работы (непрерывное добывание, сбор, изучение, отображение и анализ данных об обстановке (маркетинг, разведка, мониторинг))», так как она основана на фиксации факта проявления энергии.

«Предназначение» мы должны интерпретировать как элемент модели «решения» в виде «реализации» решения. На методическом уровне, необходимо представить причинно-следственную связь. Для этого необходимо, применяя метод абстрагирования, интерпретировать математической категорией «обстановку» (модель объекта), «информационно-аналитическая работа» (модель действия), «реализация» (предназначение).

Предлагаемый аппарат позволяет построить модель управленческого решения и на основе этого увязать три важнейших процесса в организации. За счет этой модели обеспечивается гарантия достижения выполнения плана. На основе применения закона сохранения целостности формируется концепции поддержания функционирования организации производства на основе обратной связи. За счет этого согласования снижается риск невыполнения задачи организацией.

Васильченко Д.С., Тындыкарь Л.Н., Берлова Н.М.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МОДЕЛИРОВАНИЕ ПРИ СОЗДАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ НА ПРЕДПРИЯТИИ

Как правило, создание или совершенствование информационных систем управления (ИСУ) производится в условиях действующего предприятия, когда нет возможности проверить на практике несколько проектных решений с целью выбора наиболее эффективного. Так как создание таких систем представляет собой сложную задачу, результат которой сложно предвидеть заранее, и экспертная оценка получается недостаточно точной, что приводит к большим ошибкам в оценке результатов и эффективности создаваемых систем. Одним из методов экспериментальной проверки является отработка разрабатываемых вариантов, включающая выделение предприятия и построение основного макета, однако, такой метод не всегда оправдан.

Обращаюсь к опыту создания сложных технических систем в промышленности, где имеется ряд эффективных методов проверки и отработки проектных решений, применительно к рассматриваемой проблеме можно воспользоваться методом моделирования с применением компьютерной системы, которая может стать эффективным средством проверки отработки тех или иных вариантов ИСУ до реализации непосредственно в условиях действующего предприятия. Моделирование как метод исследования будет включать два этапа:

– построение модели;
– изучение модели путём экспериментального исследования её поведения в имитируемых с помощью компьютерной системы условиях действующего предприятия.

Понятие «модель» должно использоваться только в общепринятом смысле, когда под моделью понимают вспомогательный объект, заменяющий изучаемый объект или систему, обладающий сходными с ним характеристиками и создаваемый для получения новой информации об изучаемом объекте. В связи с этим под моделью информационной системы управления на предприятии следует понимать модель, отражающую сущность научного процесса управления в конкретных условиях предприятия. Стоит отметить, что применение экономико-организационной модели позволяют чётко сформулировать хозяйственный механизм управления, решение вопросов целесообразного формообразования в управляемой и управляющей системах, их функциональные связи и зависимости.

Демидова Н.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)

ОПТИМИЗАЦИЯ СОЗДАНИЯ ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ ДЛЯ ПРОИЗВОДСТВА ФЕРРИТОВ

На любом промышленном предприятии, в том числе и на производстве ферритов, невозможно обойтись без технологического оборудования (ТО), которое участвует в производственном процессе для осуществления определённой технологии. ТО используется различными предприятиями и предназначено для оптимизации производства. Так, например, чтобы создать оборудование для обжига шихты – туннельную печь, необходимо, рассчитать параметры, нарисовать эскиз печи и сделать её чертёж. В осуществлении поставленной задачи помощником инженеру и проектировщику послужит персональный компьютер, с установленными на нём программами, а именно: Mathcad, AutoCAD и КОМПАС-3D.

С помощью программного обеспечения Mathcad инженер без труда может выполнить любые расчёты. Достоинствами программы являются: подлинные математические обозначения; мощные возможности обработки и передачи информации, которые позволяют быстрее завершать важные процессы разработки и конструирования изделий; также можно легко вводить формулы, текст, данные и изображения в одном документе, что упрощает сбор информации, повторное использование данных и верификацию проектов; помимо этого, в Mathcad ведется проверка единиц измерения – программа не позволит сложить или вычесть выражения с единицами измерения разных, по смыслу, физических величин – например, Mathcad не позволит сложить длину и массу; кроме этого, программа позволяет пользователю создавать максимально документированный расчет, использовать шаблоны.

Программы AutoCAD и КОМПАС-3D помогают проектировщику выполнить чертежи, что оптимизирует его работу. Данные программы обладают рядом преимуществ по сравнению с чертежом, нарисованным от руки: моделирование изделий, используя уже готовые компоненты либо создавая компоненты в контексте конструкций, либо комбинируя эти два способа, что обеспечивает легкую модификацию получаемых моделей; неверно начерченный элемент можно без труда стереть и, при этом не испортить чертёж или эскиз; можно вычертить отдельные элементы конструкции или полностью оборудование; специальные средства программы, упрощают работу с большими конструкциями; кроме того, возможно изменение на любом из этапов проектирования параметров элемента, вызывающее перестроение сразу же всей модели.

Таким образом, из вышесказанного можно сделать вывод, что информационные технологии значительно помогают инженеру и проектировщику в кратчайшие сроки выполнить верные расчёты, сделать аккуратные эскиз и чертежи, сэкономив при этом время.

Елисеева Ю.А., Ширяевская В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

ФУНКЦИОНАЛЬНО-СТОИМОСТНОЙ АНАЛИЗ КАК МЕТОД ОПТИМИЗАЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРЕДПРИЯТИИ СОЦИАЛЬНО-КУЛЬТУРНОЙ СФЕРЫ

В последние годы прослеживается все возрастающий интерес экспертов к методу функционально-стоимостного анализа (ФСА). Связано это с тем, что он охарактеризовал себя как результативный метод инженерной деятельности, с помощью которого удается довольно быстро и с наименьшими затратами выявлять экономически оптимальные технические решения.

Развитие и применение теории ФСА нашло обширное приложение в отраслях машиностроения, электротехнической и электронной промышленности, кинопромышленности, производства вычислительной техники, а также отрасли информационных технологий. Это связано с системностью метода, ставящего своей задачей в каждом конкретном случае выявить структуру рассматриваемого объекта, разложить его на простейшие элементы. В силу своей комплексности ФСА позволяет

выявить в каждом изучаемом объекте причинно-следственные связи между качеством, эксплуатационно-техническими характеристиками и затратами.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

О ПРЕДЕЛЬНЫХ ВОЗМОЖНОСТЯХ СООРУЖЕНИЙ, ЗАЩИЩАЮЩИХ САНКТ-ПЕТЕРБУРГ ОТ НАВОДНЕНИЙ, И НЕОБХОДТИМОСТИ РЕГУЛИРОВАТЬ СТОК РЕКИ НЕВЫ

В декабре 2015 года был большой шторм и впервые затворы судопропускных сооружений дамбы были заперты на 40 часов, хотя угроза наводнения сохранялась более двух суток. В связи с всемирным потеплением время действия нагонной волны будет возрастать и дамба не справится с задачей предотвращения наводнений в городе, если не принять соответствующих мер. Необходимо срочно начать проектирование и строительство плотин и гидростанций у истока Невы из Ладоги и у Ивановских порогов. Нева – очень полноводная река и только перекрытием этого потока на время нагонных наводнений можно уменьшить вероятность затопления города. Для начала этих работ имеются благоприятные условия – исток Невы разделен на две части островом, где расположена крепость Орешек, западная протока используется для интенсивного судоходства, а восточная часть только лишь пропускает воду из Ладоги в Неву, и вот прежде всего необходимо на этой протоке построить плотину для регулирования стока воды в Неву.

В советское время было осуществлено комплексное натурное моделирование этой проблемы и проведены точные количественные расчеты. Настало время реанимировать эти предпроектные исследования, разработать проекты этих низконапорных гидростанций и срочно их построить, кроме защиты города от наводнений они еще будут давать дешевую электроэнергию.

Иванов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский морской технический университет,

МОНИТОРИНГ И ДИАГНОСТИКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ОБОРУДОВАНИЯ ГИДРОЭЛЕКТРОСТАНЦИЙ

Гидроэлектростанции (ГЭС) являются важнейшим элементом энергосистемы, поскольку, кроме обеспечения выработки электроэнергии, они осуществляют покрытие пиков нагрузки, выполняют функции регулирования частоты в системе и исполняют роль аварийного резерва. Поэтому необходима высокая надёжность работы основного оборудования ГЭС и особенно гидроагрегатов. Для этой цели должен осуществляться постоянный контроль состояния гидроагрегатов. Задачей контроля является своевременное выявление дефектов оборудования для снижения риска возникновения аварийных ситуаций, продления срока службы агрегатов, снижения затрат на ремонты и сокращение времени простоя.

Лукьянова Л.М., Заболотский В.П., Федорченко Л.Н.
Россия, Калининград, Калининградский государственный технический университет
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ДВЕ ЗАДАЧИ ФОРМИРОВАНИЯ СИСТЕМЫ ЦЕЛЕЙ: АНАЛИЗ И СИНТЕЗ ЦЕЛЕЙ

Эффективность относят к интегральным свойствам целенаправленных процессов и рассчитывают с помощью таких частных свойств, как результативность, ресурсоемкость, оперативность.

Указанные частные свойства в изменяющихся целенаправленных процессах, характерных для целеустремленных систем (например, организационных), могут иметь различную значимость, не всегда устанавливаемую явно.

В некоторых формах управления свойство «результативность» наиболее значимо, в частности в целевом (и программно-целевом) это связано с ведущей ролью целей.

В процессе целеполагания у лица, принимающего решения, (ЛПР) вначале возникает образ результата функционирования организационной системы, представляющий ценность для ЛПР. На следующем этапе целеполагания этот образ отражается ЛПР в естественно-языковой формулировке цели, прежде всего содержательно.

В сложных системах целеполагание в большой мере реализуется в процессе анализа целей. Результат такого анализа – иерархическая аналитическая структура целей (АСЦ).

В традиции, восходящей к методу ПАТТЕРН, АСЦ называют «деревом целей». При этом как сам анализ, так и его результат в значительной степени субъективны – зависят от системы ценностей ЛПР, его генетических программ, интуиции, психических механизмов (мышление, предвидение, ценностное оценивание, эмоции и др.), ресурсов (воля и др.) и явлений (ориентационных, мотивационных и др.).

Следствия такой субъективности – возможная ложность целей, логическая некорректность и неполнота «дерева целей», выявляемые во время или даже после целедостижения, и цена

устранения соответствующих просчетов в АСЦ часто оказывается слишком высокой (в организационно-технических комплексах производственной сферы – до 10 % от общей стоимости затрат на целедостижение).

В случае некорректного АСЦ показатели ресурсоемкости и оперативности достижения целей (намечающих осуществление не совсем тех или совсем не тех результатов функционирования организационной системы) вообще вряд ли имеет смысл оценивать, что позволяет говорить о приоритетности показателя «результативность» в группе частных свойств эффективности целенаправленных процессов при любой форме управления ими.

Одним из авторов этого доклада предложен возможный путь решения проблемы некорректности АСЦ сложной системы, состоящий в дополнении процесса анализа целей явно реализуемым их синтезом, результатом которого является сетевая синтетическая структура целей, или структурная схема целедостижения (ССЦ).

Диалектически единый процесс формирования взаимообусловленных АСЦ и ССЦ (вместо традиционного «дерева целей») создаст возможность для обеспечения системности (логической корректности и полноты) целей за счет «перецелеполагания», реализуемого во взаимообратном по отношению к анализу целей процессе их синтеза).

Учитывая, с одной стороны, тот факт, что результативность целенаправленных процессов зависит от системности целей сложных объектов, а с другой – слабую формализуемость целеполагания вследствие его недостаточной изученности и трудностей объективирования, по предложенному пути решения проблемы корректности целей логично двигаться в направлении разработки методов анализа и синтеза целей конкретных классов систем и сфер деятельности.

В докладе рассматривается методы анализа и синтеза целей применительно к классу организационно-технических комплексов производственной сферы.

Лукьянова Л.М., Федорченко Л.Н.
Россия, Калининград, Калининградский государственный технический университет
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ФОРМАЛИЗАЦИЯ ГРАММАТИК И ЯЗЫКОВ ПРОБЛЕМ И ЦЕЛЕЙ КОМПЛЕКСНЫХ СИСТЕМ ПРОИЗВОДСТВЕННОЙ СФЕРЫ

Формирование решений по организационно-техническим комплексам производственной сферы (ОТК) сопряжено с трудностями, обусловленными сложностью данных объектов и недостаточной познаваемостью их свойств и поведения.

Для лиц, принимающих решения (ЛПР), трудности возрастают в проблемных ситуаций, возникающих в комплексах и окружающей среде. Неопределенность знаний ЛПР о данных объектах и большой вес субъективных моделей в методах коллективного формирования системы решений являются основными причинами позднего выявления несистемности решений по комплексам. С учетом фондоемкости данных систем несвоевременная корректировка решений, не удовлетворяющих критерию системности, влечет издержки и снижает эффективность функционирования комплексов.

В условиях неопределенности вес субъективных моделей особенно велик на начальном этапе выработки решений по ОТК – при анализе целей и проблем.

Неформализованность средств анализа целей, приводящая к противоречивости и неполноте его результатов, делает актуальным в качестве первого шага решения поставленной задачи исследование моделей формулировок целей и проблем и построение на их основе соответствующих частично формальных грамматик и языков.

Выбор класса частично формального языка целей/проблем. Анализ представительной выборки формулировок проблем и целей ОТК подтвердил выработанное В.Л Тамбовцевым положение о том, что цели (во всяком случае, из нашего опыта, их предварительные формулировки) могут быть получены путем «отрицания» соответствующих проблем.

С учетом определений понятий «цель» и «проблема» было показано, что лексически, синтаксически и семантически языки целей и проблем схожи, а принципиальным их отличием являются значения имплицитно используемого в них показателя ценности: положительной ценности (язык целей) и отрицательной (язык проблем).

Этот результат позволил не только выбрать единую частично формальную грамматику языка проблем/целей, но и создал возможность объективирования целей путем формального преобразования соответствующих проблем.

Фреймовая модель цели/проблемы. Наличие в формулировках проблем и целей эквивалентных контекстных частей утвердил нас во мнении о формальной схожести языков проблем и целей, а дальнейший анализ показал недостаточность свойств классов формальных грамматик по Н. Хомскому для их реализации.

В связи с этим были проанализированы КЗ-языки и языки представления знаний и выбран наиболее рациональный для представления знаний о целях/проблемах и удобный для ЛПР класс фреймовых языков.

Модель слота фрейма цели/проблемы. Потребовалось создание специфических фреймовых моделей целей/проблем. Однако это, наряду с некоторыми дополнительными обстоятельствами, привело к возможности разработки соответствующей двухуровневой КС-грамматики с реализацией в ней частичного учета контекста (обобщенной семантики целей/проблем).

Грамматика и частично формальный язык проблем/целей. Известно, что формальный язык относят к типу X, если существует хотя бы одна грамматика соответствующего типа, которая порождает данный язык. При разработке языка, в распознавании цепочек которого возникают трудности разбора, естественно стремление без потери его мощности перевести реализуемый язык из класса X в класс Y, например, из класса КЗ-языков в класс КС-языков, для которых отработаны алгоритмы разбора. Перевод осуществляется посредством эквивалентных преобразований грамматики исходного языка.

В данном контексте на основе предложенных фреймов проблемы и цели были разработаны соответствующие КЗ-грамматики с частичным учетом прагматики и семантики проблем и целей и осуществлен перевод их в эквивалентные двухуровневые КС-грамматики. Первый уровень определяет структуру предложения-проблемы/предложения-цели, а второй – структуру его ролевой фразы.

В докладе приводятся грамматики и построенные на их основе частично формальные языки с формализованной обобщённой семантикой проблем и целей. Проверка данных языков в диалоге ЛПР с прототипом системы поддержки принятия решений по целям ОТК и самими ОТК как средствами целедостижения показало их эффективность.

Ложкинс А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПОДХОД И ТЕХНОЛОГИИ К ОПЕРАТИВНОМУ ПЛАНИРОВАНИЮ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

Объемы и масштабы современного производства приводят к тому, что организация и планирование работы требуют отдельного решения, оптимальность которого, существенно влияет на затраты производства. Составление или планирование расписаний является одной из ключевых задач организации производства. В данной работе предлагается подход к поиску точного оптимального расписания при поставленных ограничениях на основе линейного программирования.

Предлагаемый подход использует идею закона сохранения массы. Балансирующее уравнение связывает состояния объектов в различные моменты времени, что позволяет рассматривать непрерывную цепочку состояний моделируемого ресурса и связывать состояния разных объектов между собой.

Используемая концепция составления расписания производственных объектов позволяет найти нетривиальные решения с минимальным влиянием субъективных факторов. Вариативность целевой функции предоставляет возможность оптимизировать по различным ресурсным факторам.

Михайлов Н.С.
Россия, Санкт-Петербург, АО «Равенство»

АРХИТЕКТУРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

Развитие информационных систем ведет к объединению специальных систем в единую интегрированную корпоративную информационную систему. Неотемлемой частью такой системы для промышленного предприятия является система подготовки и управления производством.

Управление в простейшей форме заключается в сборе информации (данных о ходе технологического процесса), ее переработке и выводе управляющей информации для изменения хода процесса. Этот цикл происходит периодически или непрерывно и может осуществляться с помощью автоматизированной системы управления, которая выполняет все или некоторые из перечисленных операций.

Ключевым элементом системы управления производством должна быть система планирования. Источниками данных для нее служат ERP и PLM системы. Потребителями разработанных планов и расписаний являются диспетчерсие системы или MES.

Петров В.А.
Россия, Санкт-Петербург, АО «Равенство»

ОПЕРАТИВНОЕ ПЛАНИРОВАНИЕ ПРОИЗВОДСТВА.

В условиях рыночной экономики, промышленным предприятиям необходимо оперативно реагировать на изменения спроса и предложения на изготовляемую продукцию, сокращать издержки производства и не допускать простоя дорогостоящего оборудования. Для этих целей используются APS-системы.

APS – это системы синхронного оптимизационного планирования производства, которые ориентированы на интеграцию планирования звеньев цепочки поставок, учитывающие все особенности и ограничения производства. Другими словами, это то, что позволит эффективно распределить выпускаемую продукцию по рабочим центрам и заранее закупить необходимые компоненты у поставщиков.

Особенности решения APS:

- возможность применения к различным средам планирования;
- планирование закупок и производства производится одновременно с учетом ограничений по мощностям и ресурсам;
- оптимизационное планирование;
- высокая скорость создания планов;
- незамедлительное реагирование на изменение среды;
- распределенное планирование.

Для организации единого информационного пространства на предприятии APS-системы интегрируются с другими автоматизированными системами управления, такими как ERP, MES, PLM.

Рунёв Е.В., Сорокин Р.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербургский государственный университет

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ В ЗАДАЧАХ С ОГРАНИЧЕНЫМИ РЕСУРСАМИ

Одними из актуальных в настоящее время приложений теории оптимального управления является теория финансовых рынков, в частности модели управления активами в условиях ограниченности ресурсов. Классическая теория ценообразования на финансовые активы в условиях неопределенности исходит из того, что цена актива является случайным процессом в непрерывном времени, подчинённая некоторому стохастическому дифференциальному уравнению с заданным начальным состоянием.

В работе рассматривается модель, учитывающая возможность дополнительного инвестирования и реинвестирования. Так стоимость портфеля учитывает не только количество актива и его стоимость, но и инвестиционный денежный поток, выступающий в качестве функции управления. Другими словами, изменение стоимости портфеля происходит не только за счет изменения стоимости актива, но и поступающих инвестиций.

Задача сводится к поиску оптимального управления в классе кусочно-непрерывных функций, на траекториях (решениях начально-краевой задачи) некоторого параболического уравнения, где в качестве критерия оптимальности взят интегральный функционал общего вида.

Показано, что данная модель допускает обобщение: в качестве исходного параболического уравнения может выступать эволюционное уравнение с классическим оператором Штурма-Лиувилля или его обобщениями в правой части. Таким образом, указанное обобщение описывает целый класс математических моделей, основанных на стохастических дифференциальных уравнениях.

Свиньин С.Ф., Зайнитдинов Х.Н., Хамдамов У.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Республика Узбекистан, г. Ташкент, Ташкентский университет информационных технологий

СПЛАЙН-ВЕЙВЛЕТЫ И ИХ ПРИМЕНЕНИЕ В ЗАДАЧАХ ВОССТАНОВЛЕНИЯ СИГНАЛОВ ПО ДИСКРЕТНЫМ ОТСЧЕТАМ

В докладе обсуждаются вопросы, связанные с фактором конечной длительности непрерывных сигналов, поступающих на обработку после физических измерений. По проблемам ошибок, возникающих в результате усечения интерполяционного кардинального ряда, написано много статей, в которых предлагаются различные формулы оценок величин этих ошибок разной степени обоснованности. В настоящее время получили интенсивное развитие методы разложения реальных финитных сигналов по финитным базисам, таким, как базисные сплайны, вейвлет-функции, сплайн-вейвлеты.

Теоремы Котельникова-Шеннона с их утверждениями о возможности точного восстановления сигналов в виде разложения по функциям типа sinc(t) аналитического кардинального ряда противоречат установленному в физике принципу неопределенности Гейзенберга для измеряемых сигналов. В докладе приводится современная формулировка этого принципа для реальных сигналов – функций времени. Способствует улучшению оценок точности восстановления существующая классификация таких базисов, как сплайн-вейвлеты, по их отношению к признакам ортогональности: ортогональные, полуортогональные, ортогональные при сдвигах и биортогональные. Все эти классы могут найти эффективное применение в процессах формирования дискретных выборок сигналов и последующего восстановления, особенно в связи с наличием разнообразных алгоритмов быстрых алгоритмов дискретных ортогональных преобразований.

В качестве примера рассматриваются сдвиговые сплайн-вейвлеты третьей степени (кубические) порядка 4, заданные на компактных носителях. B-сплайны определяются рекурсивно, начиная с порядка 1. Задачи восстановления сигналов по системам финитных базисных функций могут решаться как интерполяционные и как сглаживающие аппроксимации с применением фильтров различных порядков. Для восстановления сигнала важную роль играют выражения для спектральных плотностей в смысле обобщенных рядов Фурье базисных функций и критерии близости восстанавливаемых рядов восстановления в энергетических пространствах.

С применением теоремы Планшереля выведено аналитическое выражение для разности энергии восстановленного сигнала и полной его энергии, определенной в исходном пространстве функций времени. С уменьшением шага выборки имеет место асимптотическая сходимость. Процесс сходимости показан на примерах таких сигналов низкой частоты, как электрогастрограммы. Их типовые записи имеют большие длительности (порядка 40 минут), значительно превышающими, например, записи электрокардиограмм и электроэнцефалограмм.

Цехановский В.В., Чертовской В.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

СИСТЕМНОЕ ПРИМЕНЕНИЕ ЗАДАЧИ СТАТИЧЕСКОГО ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ В АДАПТИВНОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

Новый класс адаптивных систем управления производством позволяет работать при изменении состава вектора цели в процедуре функционирования]. Для такой системы характерна трехуровневая структура «руководитель – диспетчер – начальники цехов». Для функционального наполнения структуры предложен однородный метод. Основным локальным алгоритмом метода является известная задача (статического) линейного программирования (СЛП). В настоящее время имеется значительное количество исследований задачи СЛП для отдельного структурного элемента

Рассмотрены системные свойства задачи статического линейного программирования при исследовании процесса планирования в трехуровневой адаптивной системе управления производством. Рассмотрены теоретический и прикладной аспекты. В прикладном аспекте представлены вопросы компьютерной реализации моделей малой и высокой размерности.

Выделены теоретический и прикладной аспекты формирования оптимального решения.

В теоретическом аспекте рассмотрим следующие возможности СЛП:

1) Задача динамического линейного программирования (ДЛП). Внешняя рыночная среда, в которой работает система, характеризуется высокой динамичностью, что определяет динамичность процесса планирования. Для его описания задача СЛП дополняется системой разностных уравнений и обращается в задачу ДЛП.

2) Согласование экономических интересов. Экономические интересы отражаются целевыми функциями структурных элементов. В работе [2] показано, что уровни структуры согласованы между собой, а для элементов среднего уровня предложен алгоритм согласования.

3) Использование методов исследования активных систем. Безусловный интерес представляют для адаптивной системы в части выработки решений многочисленные активные методы Большинство из них, называемых технологиями, опираются на оптимальные задачи статического линейного программирования. Огромным достоинствами активных технологий является формализация решений, связанных с «человеческим фактором». Игровые приемы позволяют учитывать активность руководителей при принятии решений.

Прикладной аспект предполагает изучение вопросов компьютерной реализации системы:

1) генерация числовых данных;.

2) свойства задачи СЛП;

3) соотношение задач СЛП в процедуре генерации числовых данных;

4) переход на выпуск новой продукции с пересчетом плана;

5) реализация трехуровневой системы.

Выявлены новые теоретические и прикладные возможности задачи СЛП, которые позволяют моделировать процессы планирования в многоуровневых адаптивных автоматизированных системах управления производством сучетом интеграции экономических и динамических свойств. Дальнейшие работы в исследовании системных моделей следует проводить в уточнении алгоритма генерации числовых данных верхнего уровня, поиска новых методов исследования многоуровневых систем.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

Бабуров В.И., Васильева Н.В., Иванцевич Н.В.
Россия, Санкт-Петербург, АО «ВНИИРА-Навигатор»

ИССЛЕДОВАНИЕ ТОЧНОСТИ НАВИГАЦИОННЫХ ОПРЕДЕЛЕНИЙ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПО СИСТЕМЕ ГЛОНАСС И ПСЕВДОСПУТНИКАМ В АРКТИЧЕСКОМ РЕГИОНЕ РОССИИ

Интенсивное освоение Арктического региона России предполагает существенное увеличение интенсивности полетов различных типов летательных аппаратов (ЛА) в регионе и использование для их посадки необорудованных традиционными посадочными средствами площадок и ледовых аэродромов. Это определяет актуальность задачи навигационного обеспечения ЛА на всех этапах полета в Арктике, включая и режим посадки. С учетом того, что навигационные системы с наземным базированием имеют ограниченные зоны действия, не покрывающие Арктический регион полностью, и значительно уступают в точности спутниковым радионавигационным системам, применение спутниковой навигационной аппаратуры для навигации и посадки является перспективным.

Однако особенности функционирования спутниковых приёмников в Арктике, обусловленные специфическими свойствами арктических трасс распространения спутниковых навигационных сигналов, наличием геомагнитных аномалий и значительных отражений радиосигналов от подстилающей поверхности, затрудняют использование стандартных модификаций навигационной аппаратуры. Влияние этих негативных факторов может быть в значительной степени ослаблено, если использовать специальные алгоритмы выбора рабочих созвездий навигационных спутников, составленные с учетом информационной избыточности навигационного поля ГЛОНАСС или интегрированного навигационного поля ГЛОНАСС и локальных наземных радионавигационных точек, например, псевдоспутников.

В докладе анализируются состав рабочих созвездий и характеристики точности местоопределений по системам ГЛОНАСС и интегрированной навигационной системе на основе ГЛОНАСС в Арктическом регионе России. Исследования выполнены методом имитационного математического моделирования. Установлена значительная избыточность рабочих созвездий при номинальном значении допустимого угла возвышения спутников. Исследована возможность использования этого фактора для снижения влияния многолучевости на точность местоопределений в бортовом навигационно-посадочном комплексе.

Белоусов С.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО СПОПОСБА ОБРАБОТКИ ГРАФИКА ТОКА ПЕРЕВОДА СТРЕЛОЧНОГО ПЕРЕВОДНОГО УСТРОЙСТВА С ЭЛЕКТРОДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА ДЛЯ ДИАГНОСТИРОВАНИЯ НЕЙРОННОЙ СЕТЬЮ

При использовании нейронных сетей для задач классификации результат работы зависит от способа обработки входных данных. Простейшим способом для задач классификации графиков является выбор структуры сети с таким количеством нейронов входного слоя, которое равно числу отсчётов графика, и направление на вход сети всех значений графика. В диссертации Бочкарева С.В. «Методы диагностирования и прогнозирования технического состояния стрелочного переводного устройства» было показано, что качество диагностирования можно существенно увеличить, если вместо всех значений графика тока перевода подать на вход сети значения нескольких диагностических параметров, рассчитанных для каждого графика.

Очевидно, что существуют разные способы обработки входных данных для этой задачи, некоторые из них могут показать больший процент верно классифицированных состояний. В настоящей работе было проведено сравнение трёх вариантов входных данных: диагностических параметров, спектра графика тока перевода и комбинации этих вариантов.

На вход нейронной сети в виде диагностических параметров подавались следующие значения:

- среднее значение тока в рабочей зоне;
- дисперсия значений в рабочей зоне;
- среднее отклонение следующего значения от предыдущего;
- угол направления графика рабочей зоны;
- количество значений в рабочей зоне;
- число экстремумов графика рабочей зоны;

- число локальных минимумов графика экстремумов рабочей зоны;
- число локальных максимумов графика экстремумов рабочей зоны.

Спектр графика тока перевода был получен с помощью алгоритма прямого дискретного преобразования Фурье, который был применен к рабочей зоне графика тока перевода. Для того, чтобы получать спектр с требуемым количество значений независимо от длительности перевода, было принято решение привести все графики рабочей зоны перевода к одной длине в 400 значений. Если число отсчётов в рабочей зоне превышало эту длину, график обрезался, если это число было меньше 400, то оставшиеся отсчёты заполнялись нулями. Граница в 400 значений была выбрана, потому что более 95% исследуемых графиков имели длину рабочей зоны менее 400 отсчётов. Так как в результате работы алгоритма прямого дискретного преобразования Фурье спектр получается зеркальным, то можно сократить число входов в нейронную сеть вдвое без потери полезной информации.

При комбинации описанных подходов на вход нейронной сети подавались 8 диагностических значений и 200 значений спектра.

При всех способах обработки входные данные были нормализованы, чтобы на вход нейронной сети подавался вектор X с длиной |X|=1; все сети обучались на обучающей выборке из 37049 примеров. Опытным путём была выбрана структура нейронной сети с двумя скрытыми слоями, что позволило существенно сократить время на обучение сетей по сравнению с структурой сети с одним скрытым слоем. Проверка качества работы сетей осуществлялась на тестовой выборке, не совпадающей с обучающим набором, состоящей из 476 примеров

В результате было установлено, что при использовании входных данных в виде диагностических параметров было верно распознано 70% примеров; в виде спектра графика рабочей зоны было верно распознано 75% примеров; при комбинированном подходе – 64% примеров. Таким образом, применение входных данных в виде спектра показывает лучшие из трёх приведенных вариантов результаты.

Грошев В. А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ОСОБЕННОСТИ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ВЫСОКОСКОРОСТНЫХ МАГИСТРАЛЯХ МИРА

Последовательное развитие сети высокоскоростных железнодорожных линий в стране требует пересмотра подходов, сложившихся в сфере ЖАТ. Анализ мирового опыта строительства и эксплуатации ВСМ позволит выявить основные особенности принимаемых при построении организационных и технических решений и избежать ошибок, сделанных в других странах. С этой точки зрения интересен результат работы Японии, стран Западной Европы, Китая и США.

Старейшая высокоскоростная магистраль в мире Синкансэн была запущена 1 октября 1964г., соединив станции Токио и Син-Осака. В 1995 году на линии была введена в эксплуатацию система COSMOS, обеспечивающая руководство работой и информационный обмен между диспетчерским персоналом. Железная дорога Синкансэн является обособленной высокоскоростной магистралью, для управления которой недостаточно информации только о местоположении подвижных единиц, необходимы данные о состоянии инфраструктуры, планах работы и т.д.

Европейская система ERTMS/ETCS, разрабатываемая с начала 90х годов прошлого века, призвана обеспечивать не только безопасность движения поездов, но и эксплуатационную совместимость оборудования дорог различных европейских стран с различными условиями движения. Разработкой и внедрением системы занимается консорциум UNISIG. В основе системы лежит обеспечение управления движением поездов по радиоканалу. необходимо также отметить возможность подбора состава оборудования для участков с различными характеристиками, т.н. уровни ERTMS/ETCS.

Китай, будучи одной из крупнейших стран мира по экономике и площади территории, разрабатывает собственную систему управления железнодорожным транспортом – CTCS, которая будучи аналогом европейской системы управления поездами, отличается по числу уровней и составу оборудования.

В Соединенных Штатах Америки высокоскоростное пассажирское движение развито очень слабо в сравнении с авиасообщением, что подтверждается данными по объемам перевозок. Тем не менее, в последние годы производится разработка системы PTC (Positive Train Control) под руководством FRA (Federal Railway Administration), в основе которой лежит управление по радиоканалу.

В результате исследования нормативно-правовых и технических материалов по системам управления движением высокоскоростных поездов, можно выделить следующие особенности: отказ от светофорной сигнализации, дифференциация состава оборудования в зависимости от характеристик участка, применение радиоканала в управлении, внедрение комплексных систем

управления участками, применение систем анализа информации, централизация и концентрация управления на участках.

На основе вышеизложенного можно сделать вывод, что развитие современных систем ЖАТ ведется в двух направлениях: совершенствование технических способов обеспечения управления и безопасности на железнодорожных линиях при повышении скоростей движения и объединение систем управления с информационными системами, призванное упростить процесс обмена информацией и принятия решений.

Ефанов Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ОБ ОСОБЕННОСТЯХ СИНТЕЗА ГЕНЕРАТОРОВ МОДИФИЦИРОВАННЫХ КОДОВ С СУММИРОВАНИЕМ С ПОСЛЕДОВАТЕЛЬНОСТЬЮ ВЕСОВЫХ КОЭФФИЦИЕНТОВ, ОБРАЗУЮЩЕЙ НАТУРАЛЬНЫЙ РЯД ЧИСЕЛ

В задачах технической диагностики дискретных систем часто используют классические коды с суммированием (коды Бергера) и их различные модификации. Модифицированные коды с суммированием обладают улучшенными характеристиками обнаружения ошибок, что позволяет их эффективно использовать, например, при организации систем функционального контроля комбинационных логических устройств.

Одним из эффективных способов построения модифицированного кода с суммированием является следующий подход. Разрядам информационных векторов, начиная с младшего разряда, приписываются весовые коэффициенты, образующие натуральный ряд чисел. Подсчитывается суммарный вес единичных информационных разрядов, а затем определяется наименьший неотрицательный вычет данного числа по модулю $M = 2^{\lceil \log_2 (m+1) \rceil - 1}$, где m – длина информационного вектора. Полученное число представляется в двоичном виде и записывается в младшие разряды контрольного вектора. Старший же разряд контрольного вектора определяется как сумма по модулю 2 значений разрядов, занимающих четные позиции в информационном векторе и имеющих четные значения весовых коэффициентов. Получаемый таким образом модифицированный код с суммированием имеет $k = \lceil \log_2 (m+1) \rceil$ контрольных разрядов (как и у кода Бергера), но при этом имеет минимальное общее количество необнаруживаемых ошибок при заданных значениях длин информационных и контрольных векторов и уменьшенное количество необнаруживаемых ошибок малых кратностей.

Одним из неисследованных ранее вопросов в теории модифицированных кодов с суммированием для систем технического диагностирования является синтез их генераторов (кодеров или шифраторов).

Предложенный алгоритм предполагает при синтезе использование стандартных функциональных схем сумматоров по модулю 2, полусумматоров и полных сумматоров. При этом получаемые структуры генераторов модифицированных кодов с суммированием являются простыми и по сложности сравнимыми с генераторами классических кодов Бергера.

Ефанов Д.В., Щагина В.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

КОД С СУММИРОВАНИЕМ ЕДИНИЧНЫХ РАЗРЯДОВ НА ОСНОВЕ ПРИНЦИПА ВЫДЕЛЕНИЯ ГРУПП РАЗРЯДОВ И ИХ КОНТРОЛЯ ПО МОДУЛЮ 4

При организации дискретных систем автоматики и вычислительной техники с обнаружением отказов часто применяются помехоустойчивые коды с небольшой избыточностью и простыми правилами построения. Это позволяет строить устройства с небольшими аппаратурными затратами. Часто при решении таких задач используются классические и модифицированные коды с суммированием.

Классические коды с суммированием, или коды Бергера, содержат в контрольном векторе двоичный эквивалент десятичного числа, равного сумме единичных разрядов в информационном векторе (равного весу r информационного вектора). Такие правила построения кода предполагают наличие одного и того же контрольного вектора у C_m^r информационных векторов (m – длина информационного вектора). В зависимости от значения r количество информационных векторов с одинаковыми контрольными векторами варьируется и является минимальным при r=0 или r=m и максимальным – для значений r, близких к величине $\frac{m}{2}$. Неравномерность распределения информационных векторов между контрольными определяет высокое количество необнаруживаемых

кодом Бергера ошибок. Кроме того, поскольку $r \in [0; m]$, для всех кодов Бергера с длинами информационных векторов $m \neq 2^i - 1,$ i=1,2,… невозможно формирование полного множества контрольных векторов. Это является проблемой при решении задачи обеспечения самопроверяемости генератора кода в системах критического значения.

Коды Бергера неэффективно используют свои контрольные разряды. Можно предложить способ улучшения характеристик кодов Бергера за счет следующего алгоритма.

Получаемый таким образом код всегда будет иметь 4 контрольных разряда и может быть сравним с кодом Бергера при длинах информационных векторов m=8÷15. На данных длинах информационных векторов описываемый код будет иметь существенное преимущество в обнаруживающей способности перед кодом Бергера.

Анализируя свойства кода, строящегося по приведенному алгоритму, можно сделать вывод о том, что данный код более чем в два раза эффективнее обнаруживает двукратные ошибки, чем код Бергера, что может быть учтено при организации систем с обнаружением неисправностей. Для данного кода также гораздо проще обеспечить свойство самопроверяемости генератора. Тем не менее, код не лишен недостатков – в отличие от кодов Бергера им не обнаруживается некоторое количество монотонных ошибок в информационных векторах. Полученные теоретические результаты дополняются результатами экспериментальных исследований с системой контрольных комбинационных схем LGSynth`89 по организации систем функционального контроля по описанному коду в сравнении с приложением кодов Бергера. Эксперимент подтверждает эффективность предлагаемого подхода.

Ефанов Д.В., Лыков А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

СОВЕРШЕНСТВОВАНИЕ СХЕМНЫХ РЕШЕНИЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ЖЕЛЕЗНОДОРОЖНЫХ ПЕРЕЕЗДАХ ПРИ ОРГАНИЗАЦИИ ВЫСОКОСКОРОСТНОГО СООБЩЕНИЯ

Большое количество транспортных происшествий происходит на железнодорожных переездах, что связано с особенностями их расположения – железная и автомобильная дороги пересекаются в одном уровне. С целью повышения уровня безопасности движения как поездов, так и автомобилей переезды оборудуются специализированными устройствами ограждения и сигнализации.

В настоящее время на железных дорогах России для проектирования схем сигнализации применяются типовые решения 410407-ТМП «Схемы переездной сигнализации для переездов, расположенных на перегонах при любых средствах сигнализации и связи АПС-04». Данные технические решения предполагают использование алгоритмов последовательного занятия и освобождения рельсовых цепей, а также предполагают выдержку времени на блокирование участков удаления, позволяющую производить открытие переезда за хвостом поезда при освобождении переезда. Для открытия переезда за хвостом поезда используется двухкаскадная схема блокирования, построенная с устройствами выдержки времени за счет блокирующих реле, для которых обеспечивается требуемое замедление на отпадание якоря при помощи конденсаторов. Применение двухкаскадной схемы блокирования позволило отказаться от схемы сброса, так как через определенное время схема переезда приходила в исходное состояние и позволяла закрывать переезд независимо от направления движения поезда. Практические же результаты использования данных схемных решений показали, что временные параметры блокирования второго каскада, рассчитанные на скорость движения поезда до 50 км/ч, при уменьшенных скоростях приводят к повторному закрытию переезда, что является причиной длительного закрытого его состояния.

С целью совершенствования схемных решений железнодорожной автоматики и телемеханики было проведено моделирование поведения всех схем, отвечающих за работу переездной сигнализации, в специально разработанной на кафедре «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения среде моделирования релейно-контактных схем. В данной среде все принципиальные схемы железнодорожной автоматики изображаются из библиотечных элементов (реле, контакты, лампы и пр.), имеющих наборы характеристик согласно действующим стандартам и позволяющим учитывать все особенности реальных схем железнодорожной автоматики. В процессе моделирования были проведены следующие действия:

– построена схема фактического направления движения (она позволяет определять фактическое направление движения поезда независимо от установленного направления движения на перегоне);

– исключена схема блокирования второго участка удаления, основанная на использовании выдержки времени при помощи конденсаторов;

– построена схема блокирования и сброса, основанная на алгоритме последовательного занятия и освобождения рельсовых цепей поездом, для чего организован дополнительный участок контроля;

– при наличии остановочной платформы в районе рельсовой цепи защитного участка время блокирования увеличено до 180 секунд (60 секунд на торможение и остановку поезда, 60 секунд на посадку и высадку пассажиров, 60 секунд на разгон и проследование поездом рельсовой цепи).

Моделирование работы схемных решений железнодорожной автоматики позволило обосновать отказ от второго каскада блокирующих реле, имеющего схемы сброса и реализующего алгоритмы последовательного занятия и освобождения рельсовых цепей поездом при освобождении переезда. Технические решения по проектированию железнодорожной сигнализации в их окончательном исправленном виде позволяют реализовывать алгоритмы работы переездной сигнализации с исключением временных параметров работы участка удаления и являются эффективным решением задачи по исключению необоснованного повторного закрытия переезда при движении поезда со скоростью 50 км/ч и меньше.

Журавлева Л.М., Ивашевский М.Р., Григорук А.А., Ефимова Н.О.
Россия, г. Москва, Московский государственный университет путей сообщения Императора Николая II

ПОВЫШЕНИЕ ТЕХНИЧЕСКОГО УРОВНЯ БАЗОВЫХ ЭЛЕМЕНТОВ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Вопросы совершенствования высокоскоростных волоконно-оптических систем передачи информации (ВОСП) являются весьма актуальными в связи со стремительным ростом объемов передаваемой информации.

Наибольшее значение в обеспечении высокого технического уровня и качества ВОСП имеет создание перспективных базовых элементов оптоэлектроники на новых физико-технологических принципах. Это относится к разработке и производству новых материалов, технологий и изделий для ВОСП.

Весьма перспективным в отличие от традиционных способ создания наноструктур является метод получения квантовых ям, проволок и точек из собственных изотопов исходных химических элементов для получения новых эффектов и оптоэлектронных характеристик. Исходные вещества (собственные изотопы химического элемента) близки по химическому составу (одинаковая электронная оболочка) и значениям постоянной кристаллической решетки. В то же время изотопы различны по физическим оптоэлектронным характеристикам (разные ширина запрещенной зоны, спины ядер, коэффициенты преломления, поглощения, магнитные свойства и т.д.).

Это позволяет создавать пространственные ограничения для наноструктур без дополнительных (легирующих) химических элементов, отрицательно влияющих на некоторые оптоэлектронные характеристики материала. Для формирования и производства изотопических наноструктур (ИНС) базовых элементов ВОСП целесообразно использование различных технологических методов изменения состава и концентрации изотопов, например, основанных на микроэлектронной технологии облучения исходного материала пучком тепловых нейтронов (нейтронное трансмутационное легирование НТЛ).

Применение НТЛ для производства таких модифицированных наноструктур обеспечит требуемое качество ИНС за счет необходимых разрешающей способности технологии и чистоты материала (без химических реакций). Отсюда, открывается возможность производить многослойные наноструктуры с шириной каждого слоя, соизмеримой с величиной постоянной кристаллической решетки. Применение материала из ИНС, характеризуемых меньшими числом каналов рассеяния и временем термализации электронов, большей продолжительностью «жизни» экситонов, позволяет значительно повысить технический уровень приемо-передающей аппаратуры ВОСП.

Зозуля А.Р.
Россия, г. Петрозаводск, Петрозаводская дистанция сигнализации, централизации и блокировки Октябрьской дирекции инфраструктуры Октябрьской железной дороги

МОДИФИКАЦИЯ АЛГОРИТМА ВЫЯВЛЕНИЯ ПРЕДОТКАЗНЫХ СОСТОЯНИЙ В СИСТЕМЕ ТЕХНИЧЕСКОГО ДИАГНОСТИРОВАНИЯ И МОНИТОРИНГА УСТРОЙСТВ АВТОМАТИКИ НА ПОЛИГОНЕ ОКТЯБРЬСКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

На данный момент в системе технического диагностирования и мониторинга (СТДМ), используемой на полигоне Октябрьской железной дороги (ОкЖД), а именно, в системе "Аппаратно-программный комплекс диспетчерского контроля" (АПК-ДК), производится контроль измеряемых параметров только за пределами определенных границ: минимальных и максимальных значений, устанавливаемых на этапе проектирования системы мониторинга. Из-за такого метода диагностирования многие неисправности остаются незамеченными. Например, при нестабильном поведение измеряемой характеристики на выходе путевого приемника (ПП) рельсовой цепи

тональной частоты или устройства контроля схода подвижного состава (УКСПС) система не сигнализирует об угрозе неисправности. Учитывая нагрузку движения на главном ходу ОкЖД (линия Санкт-Петербург – Москва) неисправности по вине дирекции инфраструктуры ОАО «РЖД» абсолютно недопустимы. При диагностировании параметров таких устройств как ПП и УКСПС не только по минимальной и максимальной границам, но и в рамках нормального состояния, ряд возможных отказов, и даже предотказов, можно предотвратить.

Изначально акцент был сделан только на подобную реализацию алгоритма для мониторинга напряжения на выходе ПП, так как больше 70% отказов с ложной занятостью приходится на пробой изолирующего стыка, вследствие чего падает напряжение на выходе ПП. Далее при сборе статистических данных по отказам дирекции инфраструктуры ОкЖД было установлено, что более 80% отказов, которые приходятся на неисправности УКСПС по вине дирекции инфраструктуры вызвано изломами стоек датчика при наличии старой трещины. То есть от больших вибраций при движении и зимой, при наличии наледи на локомотиве, УКСПС подвергается незначительному надлому, который не контролируется СТДМ. Подобные ситуации приводят к отказу, задержкам поездов и большим финансовым потерям.

Суть нововведения заключается в том, что СТДМ контролирует параметр не только по заданным границам, но и относительно своего среднего значения. При нестабильном, для своего нормального состояния поведении характеристики система сообщает об угрозе неисправности оператору (ШЧД или ШЧДМ), который сообщает о возможной неисправности электромеханику сигнализации, централизации и блокировки. В ходе оперативных действий персонала удастся снизить количество отказов в дирекции инфраструктуры, избежать возможные задержки поездов, которые недопустимы по пути проследования скоростного поезда «Сапсан». Для компании ОАО «РЖД» наличие такого метода диагностирования является отличной возможностью снизить количество отказов, устранить большое количество задержек поездов, сохранить деньги компании. Вовремя приехавший поезд - это не только большое количество сэкономленных денежных средств компании, но и ее имидж.

Учитывая тот факт, что за первую половину текущего года по вине дирекции инфраструктуры во внимание берутся такие отказы как ложная занятость рельсовой цепи и неисправность УКСПС, было задержано 153 поезда как грузового, так и пассажирского движения. Время отказов было разнообразным: от 7 минут до 6 часов 36 минут. Задержка грузовых поездов на общее время 95 часов 33 минуты, пассажирских - на 8 часов 1 минуту, поездов пригородного сообщения - на 5 часов 20 минут. Учитывая стоимость простоя поездов, дирекция инфраструктуры потеряла только на этом порядка 300 тыс. рублей, без учета оплаты труда рабочему персоналу, который в некоторых случаях выходил на устранение вне рабочего времени. Также финансовые потери дирекции инфраструктуры составили порядка 1400 тыс. руб на стоимости отказов без простоя поездов. Таким образом, за полгода был понесен убыток на вышеперечисленных отказах около 2 млн. руб. Задержки поездов пассажирского движения привели к ухудшению статуса компании в глазах потребителей.

Таким образом, при внедрении вышеописанной технологии, компания имеет возможность не только сэкономить достаточно большое количество денежных средств, повысить безопасность движения на полигоне ОкЖД, но и улучшить качество труда рабочих и повысить свой статус в глазах клиентов компании.

Плюсом данной технологии является отсутствие внедрения новых технических средств и малые затраты на усовершенствование действующего алгоритма обработки измеряемых параметров.

Исаева М.Ф., Глухарев М.Л.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ В ГЕТЕРОГЕННЫХ РАСПРЕДЕЛЁННЫХ ИСТОЧНИКАХ ДАННЫХ И ПРОБЛЕМЫ ЕЁ ОБЕСПЕЧЕНИЯ

В настоящее время активно разрабатываются информационные системы, в которых происходит как обработка структурированных данных, так и семантическое моделирование различных предметных областей. При этом наряду с традиционно используемыми реляционными базами данных (БД) широкое распространение получают БД на основе различных постреляционных моделей. В связи с этим производится интеграция баз данных, использующих различные модели данных (реляционные, постреляционные, семантические и др.), а также происходит построение сложных распределенных источников. Следствием усложнения систем баз данных является возникновение новых угроз безопасности хранимой и обрабатываемой информации, в связи с чем, вопросы защиты информации в системах баз данных требуют все более пристального внимания.

Одним из вопросов обеспечения безопасности, который недостаточно глубоко рассмотрен в области информационной безопасности, является целостность информации. Сущностные отличия между различными моделями данных (в т. ч. касающиеся аспекта целостности) порождают проблему

обеспечения и поддержки целостности информации на уровне гетерогенной постреляционной БД в целом.

Под целостностью информации понимается свойство информации сохранять свое семантическое содержание, быть устойчивой к случайному или преднамеренному искажению, разрушению. Наряду с доступностью и конфиденциальностью, целостность должна обеспечивать безопасность информации в различных источниках данных.

Для обеспечения данного свойства информации в базах данных применяются различные модели политики информации – формальное представление политики безопасности для определения системы или класса систем, выполняющих обработку, хранение, распространение и защиту информации.

К целостности формальное правило чаще всего определяет следующие требования:

обеспечение защиты информации от нелегальных действий в процессе хранения, обработки и передачи (в отношении данных);

отсутствие двойственности в работе системы (целостность системы).

Наряду с доступностью и конфиденциальностью, целостность, должна обеспечивать безопасность информации в различных источниках данных.

Под безопасностью базы данных следует понимать состояние защищенности, обеспечивающее целостность, конфиденциальность и доступность хранимых данных, устойчивость функционирования систем управления базами (СУБД) данных в условиях умышленных и неумышленных воздействий дестабилизирующих факторов.

Нарушение целостности приводит к тому, что пользователь во время работы с программной системой получает некорректную информацию о чем-либо, что оказывается источником серьезных проблем на производстве.

С точки зрения развития систем с элементами интеллектуализации рассматриваются активные базы данных. База данных называется активной, если система управления базой данных (СУАБД) по отношению к ней выполняет не только те действия, которые явно указывает пользователь, но и дополнительные действия в соответствии с правилами, заложенными в саму БД. При этом СУАБД постоянно отслеживает наступление определенных событий, реагируя на активность системы и пользователя, и отвечают на события путем вызова процедур, затрагивающих как саму базу данных, так и ее окружение.

Для обеспечения реагирующего поведения СУАБД должна поддерживать соответствующие модели описания и выполнения правил: «Событие» (Event) → «Условие» (Condition) → «Действие» (Action). «Событие» описывает какое-либо событие, которое может произойти в СУБД или вне ее. «Условие» проверяет контекст, при котором событие произошло. «Действие» описывает процедуру, которая должна быть выполнена правилом, если соответствующее событие произошло и условие оказалось истинным.

Концепция активных баз данных (АБД) учитывает возможность наличия промежуточных элементарных событий, что означает принципиальную возможность полной проверки изменений, вносимых пользователями в логику обработки событий. В качестве обработчиков событий в активных БД используются активные правила, хранимые наравне с традиционным наполнением БД и обеспечивающие реагирование на события без необходимости в командах от внешнего приложения.

Таким образом, в ходе исследования проблемы представляют интерес следующие задачи: разработка способа построения моделей требований целостности, которые будут рассматриваться как разновидность активных правил (метамодель целостности, охватывающая несколько моделей данных); разработка методов реализации активных правил, а также разработка методов верификации.

Калинин В.М.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ИСПОЛЬЗОВАНИЕ СТОХАСТИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ ИНФОРМАЦИИ В МЕТОДАХ ОПТИМИЗАЦИИ

В измерительной технике, радиолокации, гидроакустике часто требуется решить оптимизационную задачу по определению экстремума функции регрессии. Под методом оптимизации понимают способ, который помогает решить следующую задачу: необходимо найти максимум или минимум функции регрессии. На практике, при измерении параметров сигналов, приходится учитывать влияние случайных воздействий или помех (естественных и искуственных), которые могут накладываться на функцию. При наличии помех известна не сама функция, а некоторая функция или её градиенты. Часто приходится иметь дело с выпуклыми функциями. Наиболее перспективными и современными методами оптимизации являются методы с адаптивной регулировкой шага итерации, что позволяет быстро (по сравнению с фиксированным шагом) достигнуть окрестности точки минимума.

В докладе рассматривается краткое описание создаваемого метода оптимизации, представлена основная идея нового метода, описан алгоритм работы данного метода, а также выявлены характерные преимущества реализации алгоритма на стохастическом преобразователе код - вероятность.

Все возможные алгоритмы оптимизации можно классифицировать на различные категории, например: вероятностные – детерминированные, градиентные – неградиентные, поисковые – непоисковые. Новый метод будет вероятностным, неградиентным, поисковым. Вероятностные алгоритмы те, в состав которых входят операции, основанные на случайных явлениях. Неградиентные алгоритмы используют оценки самой функции, в то время как градиентные работают с градиентом функции, что накладывает на неё ограничения. Поисковые алгоритмы предполагают наличие случайных или не случайных проб, предназначенных для оценки текущего состояния процесса оптимизации и формирования информации, необходимой для последующего движения к точке минимума или максимума функции.

Основная идея будущего метода в наличии шагового множителя, который будет регулировать скорость приближения к точке минимума. На первом шаге работы алгоритма случайным образом выбирается вектор инициализации и определяется значение функции при данном векторе. Далее происходит смещение. Для этого к текущему вектору прибавляется приращение, состоящее из произведения шагового множителя и вектора, который принимает случайные равновероятностные значения. После этого сравниваются значения функции на предыдущем шаге и актуальное значение. Если новое значение меньше предыдущего, осуществляется переход к следующему шагу, в противном случае подбирается иное приращение.

Необходимо отметить тот факт, что современные компьютерные системы являются мощными и высокопроизводительными, однако существуют арифметические операции, такие как: умножение, деление, возведение в степень, которые достаточно трудоёмки и занимают продолжительный промежуток времени. Использование стохастического преобразователя код – вероятность позволит реализовать алгоритм, исключив трудоёмкие операции, заменив их на более простые, например: сдвиг, сложение, вычитание, сравнение чисел. В отличии от классических стохастических вычислительных устройств предполагается, что только часть информации будет представлена в виде вероятностей, а остальные значения – как числа с фиксированной точкой.

Главной целью использования стохастического преобразователя информации будет являться уменьшение времени вычисления на каждой итерации, что должно привести к уменьшению общего времени реализации алгоритма, а значит повысить скорость и эффективность работы устройств. Стохастические методы оптимизации могут быть использованы для решения самых разнообразных практических задач, в том числе в режиме реального времени в условиях помех, где требуется высокое быстродействие при обработке поступающей информации.

Киджи Д.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

КРАТКИЙ АНАЛИЗ И ОЦЕНКА РИСКОВ ПРИ ИСПОЛЬЗОВАНИИ ЭКНИС

Электронная картографическая навигационно-информационная система (ЭКНИС) – компьютерная система, отображающая электронные навигационные карты, интегрирующая информацию с датчиков различных навигационных систем. На современных судах, по резолюции ИМО А817(19), при наличии надлежащей системы дублирования может считаться выполняющей требования Правила 19.2 Главы V МК СОЛАС («Требования к оснащению судов навигационными системами и оборудованием», «Судовое навигационное оборудование и системы»). ЭКНИС являются центральной, базовой частью для современных интегрированных мостиков (автоматизированных комплексов судовождения – АКС). Входные датчики для интегрирования навигационной информации включают гирокомпас (зачастую реализована функция подключения нескольких гирокомпасов), GPS/Глонасс (глобальная система позиционирования), лаг, AIS (автоматическая идентификационная система), ARPA (система автоматической радиолокационной прокладки), НАВТЕКС и т.д.

Ограничения ЭКНИС вызываются недостаточной точностью цифрования навигационной карты, недостаточной точностью картографической информации, ошибками датчиков навигационной информации, а также ошибками вахтенного помощника при интерпретации данных. Наибольшее влияние ошибки и погрешности датчиков навигационной информации имеют на отображаемую позицию судна, на расчет характеристик его движения, а также на позицию и характеристики движения захваченных целей САРП.

Ошибки вахтенного помощника при интерпретации данных могут быть разнообразными, в том числе к ним может относиться неправильная трактовка отображаемых данных и условных обозначений, неверно выбранный масштаб отображения карты, использование неоткорректированных, либо неофициальных карт, передоверие ЭКНИС, РЛС/САРП. По статистике Регистра Ллойда, наибольшее количество аварий судов (до 80%) вызвано ошибками человека, причем 50% аварийных случаев являются навигационными авариями и происшествиями. Недостаток

информационного обеспечения, так же как и перегрузка информацией, способствует возникновению ошибок, относящихся к проявлениям человеческого фактора.

Для того чтобы обеспечить надежность системы, необходимо выполнить ряд требований к оборудованию, таких как модульный принцип построения системы, дублирование оборудования, постоянный контроль состояния системы, а также установление порядка работы системы в случае возможных отказов. В системе должна быть обеспечена аварийно-предупредительная сигнализация или индикация в случае обнаружения неисправности оборудования.

В настоящее время ЭКНИС является важнейшим навигационным инструментом, позволяющим создавать на его основе АКС – автоматизированные комплексы судовождения. К недостаткам таких комплексов относится перегрузка навигационной информацией и потеря контроля над навигационной обстановкой в случае кратковременной неисправности системы. Большинство навигационных аварий связаны с некачественным контролем позиции судна (некачественной оценкой точности ОМС), передоверием ЭКНИС, отсутствием надлежащего визуального наблюдения. Судоводителю-оператору ЭКНИС необходимо четко представлять возможные ограничения системы, помнить о риске передоверия ЭКНИС и контролировать счисление пути судна альтернативными методами (визуальными либо радиолокационными).

Клименко С.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения императора Александра I

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ ТРАНСПОРТНЫХ ПОТОКОВ

Программный комплекс предназначен для решения многофазных транспортных задач с нелинейными функциями стоимости. Такие задачи часто возникают на практике, более того, практически во всех транспортных задачах, возникающих в транспортной логистике, зависимости стоимости транспортировки от величины перемещаемого груза являются нелинейными, что не позволяет непосредственно использовать классические алгоритмы для её решения.

Другой пример - задачи информационного регулирования потоков автомобильного транспорта: благодаря появлению в автомобилях навигационного оборудования и использованию интернета, автомобилистам открывается возможность оценивать текущее состояние сети дорог и выбирать оптимальный маршрут движения с учётом этого состояния. Таким образом, автомобилист может в готовом виде получить оптимальный по времени маршрут следования и передвигаться по нему при помощи навигатора. Но, если в качестве критерия оптимальности выбрано суммарное (или среднее по потоку) время движения от начальной до конечной точки маршрута, то алгоритмы последовательного поиска кратчайшего маршрута могут привести к далеко не оптимальному потоку. Среднее время перемещения потока по участкам транспортной сети, очевидно, зависит от величины потока на них. Эту зависимость необходимо учитывать при оптимальном распределении потока по маршрутам следования.

Подобные задачи могут быть сведены к классическим задачам (т.е. с линейной функцией стоимости) на специальным образом построенных мультисетях.

Таким образом, задача построения потока минимальной стоимости в транспортной сети играет важную роль в решении проблемы оптимизации транспортных потоков.

Разработанный программный комплекс позволяет из исходной двухполюсной сети построить двухполюсную транспортную мультисеть. В построенной мультисети число узлов соответствует исходной сети, а число дуг в мультисети, которые соответствуют дуге в исходной сети, зависит от сложности зависимости стоимости от величины потока на дуге с соответствующими начальными и конечными узлами в мультисети. После построения мультисети, на основе исходной сети, применяется модификация классического алгоритма Басакера-Гоуэна для поиска потока минимальной стоимости.

Модификация данного алгоритма заключается в том, чтобы потоки, получаемые по завершению каждой итерации, были Т-ранжированными, для этого необходимо чтобы для каждой пары дуг мультисети обратная дуга проводилась только к одной дуге из этой пары.

Основной целью дальнейшей разработки программного комплекса является визуализированная работа описанного подхода и решения задач по оптимизации транспортных потоков.

Программный комплекс разрабатывается на объектно-ориентированном языке высокого уровня C# с использованием открытой библиотеки MSAGL (Microsoft Automatic Graph Layout) от компании Microsoft. Данная библиотека позволяет визуализировать и компоновать описанную транспортную сеть. Несмотря на то, что существует большое количество открытых библиотек для визуализации сетей (графов), библиотека MSAGL имеет пару преимуществ, которые существенно выделяют ее среди других открытых библиотек:

1. Руководство по использованию.

2. Наличие примеров использования.
3. Теоретически не имеет ограничений на размер создаваемого сети(графа).

В настоящее время для решения задач по оптимизации транспортных потоков нет специализированных пакетов прикладных программ, что сильно затрудняет их решение на практике, поэтому разработка программного комплекса для решения задач оптимизации транспортных потоков является чрезвычайно актуальной.

Кокурин И.М., Тимченко В.С.
Россия, Санкт-Петербург, Институт проблем транспорта им. Н.С. Соломенко РАН

КОМПЛЕКС ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ПЕРЕВОЗОК ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТИ ОБЕСПЕЧЕНИЯ ПРОПУСКНОЙ И ПРОВОЗНОЙ СПОСОБНОСТЕЙ ЖЕЛЕЗНОДОРОЖНОЙ ЛИНИИ, ОБСЛУЖИВАЮЩЕЙ МОРСКОЙ ПОРТ

Необходимость освоения существующих, а тем более прогнозируемых объемов экспортных перевозок, требует дорогостоящей реконструкции инфраструктуры железных дорог России. Поэтому с целью сокращения инвестиций для количественной оценки пропускной и провозной способностей железнодорожных участков при сравниваемых вариантах реконструкции инфраструктуры, технических и организационных мероприятий эффективно используется разработанный и развиваемый в ИПТ РАН программный комплекс имитационного моделирования процессов железнодорожных перевозок.

Модуль планирования ремонтных работ (МПРР) комплекса на основе информации о потребной пропускной способности, пропущенном тоннаже и последнем виде ремонта пути на начало периода планирования перевозок определяет места, протяженности и длительности перерывов в движении поездов («окон»), а также ограничения скоростей поездов, обусловленные выполнением реконструктивных и ремонтных работ в соответствии с требованиями безопасности движения.

Эта информация передается в модуль имитационного моделирования процессов перевозок (ИМПП), который для заданного числа суток с использованием тяговых расчетов определяет параметры графиков моделируемого движения поездов, наличную пропускную и провозную способности.

В начале процесса моделирования пассажирские, пригородные и задаваемые пользователем грузовые поезда пропускаются по расписанию, а между ними имитируется пропуск остальных грузовых поездов. Приоритет этих поездов принимается равным доле перевозимого ими рода груза в заданном общем объеме перевозок, что гарантирует перевозку всей заданной номенклатуры грузов за сутки.

Комплекс предусматривает возможность имитации пропуска заданного или максимального количества грузовых поездов всех категорий за сутки.

В режиме пропуска заданного количества грузовых поездов они отправляются с начальных станций расчетного участка через случайные интервалы времени, формируемые по заданному закону распределения вероятностей или по расписанию.

В режиме пропуска максимального количества грузовых поездов время их появления на входе системы первоначально не задается. Поезд пропускается по железнодорожной линии в ближайший момент времени по очереди типа FIFO («первый вошел — первый вышел»).

В результате количество грузовых поездов, перевозящих всю номенклатуру грузов, которое удается пропустить за сутки при обоих максимальных режимах, становится случайной величиной, поскольку зависит от очередности поездов с различными ходовыми свойствами.

Особенность технологии работы предпортовых станций заключается в том, что длительность занятия каждого приемо-отправочного пути — это случайная величина, зависящая от даты и времени подхода морских судов, степени заполнения складов, непроизводительных простоев и других факторов, приводящих к значительному превышению нормативной длительности занятия путей. Поэтому максимальные значения длительностей занятия путей, при которых обеспечивается потребная пропускная и провозная способности железнодорожной линии, обслуживающей морской порт, определяются методом имитационного моделирования технологических процессов перевозок.

Величина наличной пропускной способности подчиняется нормальному закону распределения, что определяет формулу для оценки вероятностей освоения прогнозируемых объемов перевозок всей заданной номенклатуры грузов.

Оценки вероятностей превышения наличной пропускной способностью потребную пропускную способность для рассматриваемой железнодорожной линии определяют надежность освоения планируемых объемов перевозок при различных вариантах их организации.

Разработанный и развиваемый в ИПТ РАН программный комплекс имитационного моделирования процессов железнодорожных перевозок позволяет определять:

– ежегодную потребность и оптимальную продолжительность длительных перерывов в движении поездов («окон») на заданный период проведения ремонтных работ;

– наличную пропускную способность железнодорожного участка в реальных, а не одинаковых расчетных поездах, и провозную способность, гарантирующую перевозку заданных объемов грузов, (с учетом параметров движения всех категорий поездов, вида тяги, количества, полезной длины и длительности занятия приемо-отправочных путей, координат светофоров и длин защитных участков, используемых систем автоматики и телемеханики, наличия длительных перерывов в движении поездов);

– вероятность освоения прогнозируемых объемов железнодорожных перевозок всей номенклатуры грузов за каждый год периода планирования при минимальных объемах инвестиций.

Кушпиль И.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ЭКСПЛУАТАЦИОННО-ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ ПРИМЕНЕНИЯ СОЛНЕЧНОЙ ЭНЕРГИИ ДЛЯ ПИТАНИЯ АППАРАТУРЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Солнечная энергия приобретает популярность во многих странах, поскольку цена фотоэлементов и преобразователей для них стремительно снижается, благодаря развитию новых технологий.

В результате солнечная энергия вполне может конкурировать с энергией, получаемой из ископаемого топлива. В зонах, куда прокладка традиционных электрических сетей затруднена, солнечный свет становиться важным альтернативным источником энергии.

Устройства автоматики, телемеханики и связи в большинстве случаев потребляют не очень большую мощность. Все эти объекты могут иметь источники питания от фотоэлектрических (ФЭ) модулей. Они же могут служить и резервными источниками электропитания вместо дизель-генераторов.

В зависимости от того, в качестве чего применять (ФЭ) модули – основной электропитающей установки (ЭПУ) или резервной автономной электростанции (РАЭС), технические требования предъявляемые к устройствам электропитания ЖАТ будут различные.

В соответствии с СТО РЖД 08.025-2015, в экономически обоснованных случаях, в качестве ЭПУ и РАЭС могут использоваться альтернативные источники тока с соответствующими преобразователями.

При вводе в эксплуатацию, обслуживании и использовании (ФЭ) модулей, в качестве источника питания аппаратуры ЖАТ, возникает ряд следующих проблем:

– необходимость доработки системы питания в соответствии со стандартами и требованиями ОАО «РЖД»;

– необходимость дополнительного оборудования (АКБ, УБП, инверторов);

– проблема высокой стоимости и длительный срок окупаемости оборудования;

– наличие больших производственных площадей для размещения модулей, а также помещений для дополнительного оборудования.

Основным недостатком (ФЭ) модулей является их низкий КПД (в среднем 15%) и зависимость генерируемой мощности от времени года, времени суток, погодных условий и уровня инсоляции местности. Кроме того, перегрев модуля приводит к ухудшению его токовых показателей, что в свою очередь ведет к необходимости применения системы охлаждения.

Одной из проблем возникающей в процессе обслуживания является необходимость в регулярной очистке (ФЭ) панелей. В весенне-летний период – от пыли и птичьего помета, в осенне-зимний от снега. Это ведет к открытию новых рабочих мест, или распределению нагрузки на существующий персонал.

Кроме того, выход из строя любого фотоэлемента может привести к падению генерируемой мощности. На солнечных электростанциях, которые состоят из сотен (ФЭ) панелей, тестирование всех фотоэлементов будет очень длительной и трудоёмкой процедурой. Отсюда проблема разработки эффективных методов диагностики.

Еще одной проблемой, о которой умалчивают производители, является наличие ядовитых веществ в составе самих фотоэлементов (свинца, кадмия, галлия, мышьяка) и применение токсичных веществ, при их производстве. Как следствие после 25-30 лет эксплуатации «зеленой энергетики» возникнет проблема утилизации выработанных (ФЭ) модулей. Поэтому вопрос экологической безопасности остается открытым.

Несмотря на вышеуказанные проблемы, разработчикам фотоэлементов удается их решать. Следует иметь в виду, что в ближайшем будущем энергоемкость устройств автоматики, телемеханики и связи значительно снизится, тогда солнечные электростанции найдут широкое применения для питания этих устройств, и для энергообеспечения железнодорожного транспорта, главным образом – для отдаленных малых станций.

Марков Д.С., Соколов В.Б., Соколов М.Б.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ОСОБЕННОСТИ СИНТЕЗА МОДЕЛИ ПОРЦИОННОГО ДИНАМИЧЕСКОГО МОДЕЛИРОВАНИЯ СЛОЖНЫХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ

Предлагаемая авторами концепция синтеза модели порционного динамического моделирования (МПДМ) сложных систем массового обслуживания (ССМО), основана на понятии заявки-порции. Целью разработки МПДМ является сокращение в десятки раз затрат машинного времени на проведение серий имитационных экспериментов для операционных исследований систем данного класса по сравнению с классической формализацией имитационных моделей ССМО на основе представления заявок как единичных объектов (ЕО).

МПДМ предназначены для исследования ССМО обладающих следующими свойствами: отдельные заявки имеют малый “вес” в процессе обслуживания; количество заявок, поступающих на входы системы и находящихся в процессе обслуживания велико; количество входов и выходов системы велико; потоки заявок неравномерны во времени; интенсивность и неравномерность потоков заявок на различных входах системы различны; система обслуживания представляет собой сложную сеть с большим количеством разнородных обслуживающих устройств и накопителей; маршруты обслуживания заявок в системе разнообразны, сложны и определяются множеством логических условий разного вида.

Задачами операционных исследований таких систем являются: определение “узких мест” в процессе обслуживания заявок; оценка дефицитов (профицитов) емкостей накопителей и пропускных способностей обслуживающих устройств (ОУ) с учетом плановых ремонтов, отказов и восстановлений; определение наличия и оценка характеристик очередей заявок на входах и внутри системы. Кроме того, МПДМ должна позволять наряду с указанными выше операционными характеристиками выполнять оценку затрат времени на обслуживание заявок. МПДМ должна разрабатываться как сетевая модель ССМО основными узлами которой являются модели обслуживающих устройств (МОУ).

Заявка-порция, являющаяся основой МПДМ – это совокупность заявок – ЕО, поступающих в систему за заданный интервал времени ΔTi и рассматриваемая как единый элемент Pi; $i=\overline{1,I}$ потока, где i индекс порции по расположению на оси времени от начала моделируемого периода, причем Pi=∑pi,j; $j=\overline{1,J}$, где pi,j порция заявок, поступивших за i-ый интервал на j-ый вход, а J- количество входов в ССМО.

Разработка МОУ предполагает использование следующих параметров:

– λci,j- средняя интенсивность потока заявок за i-ый интервал по j-ому входу (среднее количество заявок ЕО в единицу времени поступающих на j-ый вход системы в течении i-го интервала);

– λm=∑ λci,j -суммарная интенсивность потока заявок ЕО на входе m-го устройства;

– Пm- производительность m-го устройства (количество заявок ЕО обслуживаемых устройством в единицу времени).

В традиционных имитационных моделях ССМО заявками являются ЕО. При этом одноканальное ОУ может быть занято только одной заявкой, а момент его освобождения определяется только временем выполнения операции данным um. Концепция МПДМ предусматривает представление в качестве заявок порций ЕО поступивших в ССМО за заданный интервал времени ΔTi, что определяет ряд специфических требований к моделям ОУ - um:

1. В многофазных ветвях сетевых моделей ССМО одна заявка-порция может одновременно занимать несколько ОУ, последовательно занимая и освобождая их в зависимости от времени выполнения операций каждым ОУ.

2. Момент освобождения u_m в многофазной ветви определяется соотношением времен выполнения операций данным и предыдущим ОУ.

3. Одноканальное ОУ могут одновременно занимать более одной $p_{i,j}$ в зависимости от соотношения суммарной интенсивности λ_m заявок-порций поступающих на вход u_m и его производительности $П_m$..

4. При одновременном обслуживании нескольких $p_{i,j}$ необходимо выполнить перерасчет времени их совместного пребывания в ОУ для каждой заявки-порции.

5. В ССМО с приведенными выше свойствами перед ОУ, как правило, имеются накопители h_z.

6. После выполнения операции каким-либо ОУ маршрут $p_{i,j}$ в сетевой модели ССМО определяется значениями ждущих α, логических q и вероятностных g логических условий, а также специфического только для порционной формализации вероятностного условия β. Условия α, q, g являются классическими, а условие β приводит к делению заявки-порции $p_{i,j}$ и его модель подлежит разработке.

В качестве инструментального средства для синтеза МПМД выбрана универсальная моделирующая система GPSS WORLD

Матушев А.А., Седых Д.В., Ушаков И.С.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

РАЗРАБОТКА ОБОБЩЕННОЙ МОДЕЛИ ПРИНЦИПИАЛЬНЫХ ЭЛЕКТРИЧЕСКИХ И МОНТАЖНЫХ СХЕМ ДЛЯ ЭКСПЕРТИЗЫ И ИНТЕЛЛЕКТУАЛЬНОЙ КОРРЕКТИРОВКИ

На сегодняшний день не существует эффективной системы проверки наличия ошибок в принципиальных электрических и монтажных схемах рассматривающих их как различные способы описание одной и той же системы. В настоящее время разработаны отраслевые форматы данных принципиальных и монтажных схем железнодорожной автоматики. Но для задач их сравнения и корректировки необходимо представление схем в виде единой модели, которая может быть построена по принципиальным или монтажным схемам.

Решение вопросов построения моделей затруднено многообразием элементов, имеющихся в железнодорожной технической документации и сложностью средств моделирования. Поэтому до настоящего времени не удавалось создать приемлемые технологии моделирования и практическую реализацию для рассматриваемых схем. Основные требования, предъявляемые к модели, с точки зрения экспертизы схем это:

1. Целостность. В процессе построения модели должны быть определены все устройства и их составляющие.

2. Полнота. Модель должна включать необходимый и точный набор логических характеристик каждого элемента.

3. Связность. Наличие устойчивых связей между элементами и их свойствами.

4. На основе приведенных выше требований была создана общая модель для принципиальных электрических и монтажных схем. Основными компонентами модели являются:

5. Рабочее пространство. Корневой элемент, содержащий в себе все элементы схемы.

6. Лист схемы, содержит в себе элементы с одного листа схемы.

7. Визуальный элемент листа схемы. Данные компоненты представляют собой все информационные фрагменты или части устройств.

8. Части устройств, представляют собой отдельные элементы различных устройств (контакты реле, обмотка реле и другие), которые в дальнейшем группируются в устройства.

9. Выводы – специальные точки устройств, входящие в состав электрического узла, определяющие место соединения нескольких элементов.

10. Электрический узел, представляет собой выводы элементов, соединенных вместе.

11. Шлюз, предназначен для описания различных переходов внутри схемы.

Для заполнения данной структуры разработан специальный алгоритм формирования модели по набору принципиальных или монтажных схем.

Разработанную модель предполагается использовать для экспертизы принципиальных и монтажных схем. Благодаря тому, что модель объединяет два вида схем можно проверить соответствие принципиальных и монтажных схем одного проекта. Помимо проверки соответствия модель позволит быстро и эффективно проверять:

1. Наименования марок приборов.
2. Соответствие контактов марке прибора.
3. Связи элементов.
4. Монтажные адреса.

Модуль экспертизы и корректировки схем с помощью предложенной модели позволит, избежать множества схемных ошибок еще на стадии проектирования. Также модуль улучшит качество работы программного комплекса распознавания МТД, корректируя полученные данные.

Ныркова А.П., Ныркова А.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ИСПОЛЬЗОВАНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ МАКСИМУМОВ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ СУДОХОДСТВА

Транспортные процессы по своей природе являются стохастическими. Для обеспечения безопасности при эксплуатации транспортных средств часто в качестве критерия или ограничений используются максимальные или минимальные значения параметров процессов, выход за пределы которых может привести к аварийным ситуациям. Например, при постановке средств навигационных ограждений на внутренних водных путях, существенным для безопасности судоходства является точность установки навигационных знаков. Предельные значения погрешности установки зависят от характеристик водного пути, степени его использования и других факторов. При осуществлении работ по постановке средств навигационных ограждений, для определения координат вычисляют среднее значение из нескольких полученных от навигационного приемника. Для того чтобы гарантировать с заданной вероятностью не превышение определенных предельных значений точности постановки необходимо установить распределение максимумов погрешностей. Зная, как ведет себя максимум

погрешности, можно снизить количество необходимых измерений, а также повысить точность постановки. Если максимальное отклонение от истинных координат установки навигационного знака не превышает предельное значение, установленное для данного участка водного пути, это означает, что можно гарантированно (с заданной вероятностью) утверждать о верной установке знака.

Из классической теории экстремальных значений известно, что если для некоторых последовательностей нормализующих констант an, bn случайная величина an(Mn - bn) имеет невырожденную предельную функцию распределения вероятностей, то эта функция должна иметь одну из трех единственно возможных форм. Здесь Mn – максимум n независимых и одинаково распределенных случайных величин.

Параметры an, bn для законов распределения вероятностей ошибок определения координат постановки навигационного знака могут быть найдены. Для составляющих компонент ошибок определения координат установки знаков установлены следующие законы распределения вероятностей: нормальный, показательный, равномерный, Рэлея и Максвелла. Для этих законов распределения вероятностей выведены аналитические соотношения параметров an, и bn.

Место выхода на точку установки знака определяется по изображению судна на электронной навигационной карте, в соответствии с координатами, получаемыми от навигационного приемника. Учитывая наличие большого числа погрешностей невозможно гарантировать попадание в точку установки навигационного знака с вероятностью близкой к 1. В реальных условиях требуется попасть в зону вокруг плавучего навигационного знака, ограниченную определенным диаметром, заданным для конкретного участка водного пути. Для того чтобы характеризовать попадание в зону вводится понятие максимума отклонения (максимума погрешности) и предельного отклонения.

Для обеспечения требуемых условий безопасности судоходства необходимо, чтобы максимум отклонения установки плавучего навигационного знака относительно заданных координат с вероятностью 0,95 не превышал определенное для данного участка водного пути предельное отклонение Mmax. Зная к какому типу распределения относится данный участок, можно определить n – минимальное количество измерений, производимых навигационным приемником в единицу времени, для обеспечения соответствующей точности.

Павлова Л.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРИМЕНЕНИЕ ПРОГРАММНОГО ПРОДУКТА ДЛЯ РАСЧЕТА ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ПРОЦЕССОВ ХРАНЕНИЯ И ПЕРЕРАБОТКИ РЕФРИЖЕРАТОРНЫХ КОНТЕЙНЕРНЫХ ГРУЗОВ

На данный момент морской порт, является крупным транспортным узлом, который включает в себя совокупность многих видов транспорта. Одним из наиболее важных объектов развития государственной экономики является портовая деятельность, и охватывает она более 50 % всего мирового грузооборота. Этому свидетельствует положительная динамика роста грузооборота морских портов России.

Для уменьшения затратной части на этапе транспортировки грузов до территории порта и сокращения времени предварительной доставки широко используются контейнерные перевозки, они отличаются очень высокой степенью безопасности. Теоретическая пропускная способность терминала не всегда совпадает с фактической. Так как техническое оборудование порта в направлении импорта и экспорта, не всегда может быть готово к хранению или обработке контейнерных грузов. В связи с этим, необходима разработка математических моделей, которые позволяют оптимизировать и уменьшить затраты на оборудование и ресурсы. Рассмотрим программный продукт, описывающий математическую модель, через систему массового обслуживания, с помощью которой возможно уменьшить погрешности при расчетах вероятностных характеристик. При использовании системы массового обслуживания Марковской модели, предполагается экспоненциальный (показательный) закон обслуживания. При расчетах вероятностных характеристик систем массового обслуживания, применение экспоненциального закона, может привести к ошибкам и недостаточной точности. Учитывая специфику контейнерных терминалов, для решения задач исследования и оптимизации, необходимо учитывать случайные процессы обработки судов, описывая эти процессы на основе вероятностных моделей. Математическая модель процесса хранения учитывает нерегулярность прихода партий грузов и случайное время нахождения их на складе в рефрижераторных контейнерных терминалах. Что приводит в одних случаях к простою оборудования и избытку мест на складах хранения, в других приводит к образованию очередей. Для того чтобы рассчитать время ожидания судна на обработку и хранение, а также определить среднее число партий контейнеров в очереди, мы введем следующие допущения: задана многоканальная разомкнутая система массового обслуживания с неограниченным временем ожидания и с неоднородным простейшим (стационарным пуассоновским) потоком требований. Неоднородный поток судов обладает различными характеристиками, т.е. разные типы судов: m1 – суда 1-го типа, m2 – суда 2-го типа, m3 – суда 3-го типа, ms – суда s-го типа; и

интенсивностью прихода грузовой партии: λ1 – для судов 1-го типа, λ2 – для судов 2-го типа, λ3 – для судов 3-го типа, λs – для судов s-го типа.

Важным параметром функционирования системы массового обслуживания является среднее время ожидания в очереди на хранение и среднее число партий контейнеров в очереди на хранении. Исходными параметрами, характеризующими систему массового обслуживания, являются:

- число условно-функциональных секций – F;
- интенсивность поступления одного требования на обслуживания - λi.
- интенсивность обслуживания суда - μ.

Используя математическую модель и схемы процессов функционирования и состояний многоканальной разомкнутой системы массового обслуживания можно рассчитать вероятностные характеристики, через программное обеспечение. Разработанное программное обеспечение представляет собой совокупность библиотек функций и динамическое содержание, направленное на произведение расчета вероятностных характеристик процессов хранения и переработки рефрижераторных контейнерных терминалов. Программа предусматривает возможность ввода параметра не имеющего количественного ограничения такого как: тип судна. Где для каждого типа судна учитываются: размер партий груза, размер (вместимость) контейнера, коэффициент заполняемости и другие характеристики для определенного типа судов.

Таким образом, полученная вероятностная модель позволяет произвести анализ процессов хранения контейнерных грузов в рефрижераторных терминалах, учитывая специфику функционирования процессов переработки грузов. При расчете математической модели, мы можем найти следующие параметры: среднее число партий контейнеров в очереди на хранение; среднее приведенное время ожидания, интенсивность прихода в терминал каждой партии контейнеров и коэффициент заполнения условно-функциональных секций. Результаты получаются точнее, чем при использовании “классического” детерминированного метода, который не полностью отражает специфику переработки рефрижераторных контейнерных грузов. За счет того, что при использовании данного метода не учитываются такие важные аспекты, как: нерегулярный поток событий, случайное время пребывания судов в терминал (в условно-функциональные секции) и случайная величина времени обработки грузов.

Пивоваров Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПОЛНОСТЬЮ САМОПРОВЕРЯЕМЫХ СТРУКТУР НА ОСНОВЕ РАВНОВЕСНОГО КОДА «1 ИЗ 4»

При построении систем функционального контроля комбинационных логических устройств остро стоит проблема обеспечения свойства полной самопроверяемости их структуры. При построении систем функционального контроля на основе метода вычисления контрольных разрядов не всегда возможно получение полностью самопроверяемой структуры, так как для выбранного кода реализация данной структуры будет единственной, что не даёт влиять на свойства системы, такие как избыточность, обнаруживающая способность и контролепригодность. В этом смысле выгодно отличаются структуры контроля по методу логического дополнения. Так как контрольные функции дополнения не определяются однозначно контролируемой схемой, то путем подбора этих функций можно обеспечить как самопроверяемость схемы, так и ее минимальную сложность. Также в структурах логического дополнения число разрядов контролируемого кода равно числу выходов схемы в отличии от структур, построенных методом вычисления контрольных разрядов, где число разрядов кода всегда больше числа выходов схемы, вследствие чего сложность тестера в структурах логического дополнения будет меньше.

При построении систем функционального контроля на основе метода логического дополнения удобно использовать равновесные коды с небольшой длиной кодовых слов. Такие коды обладают рядом преимуществ перед другими равновесными и систематическими кодами в системах функционального контроля, а именно: их тестеры имеют максимально простые структуры и для полной самопроверяемости требуют минимального количества проверочных комбинаций. Перспективным является использование равновесного кода «1 из 4» (1/4-кода). Тестер данного кода для проверки требует поступления на входы всех четырех кодовых слов: 0001, 0010, 0100 и 1000. Из современных публикаций на тему приложения 1/4-кода в системах функционального контроля следует, что для обеспечения полной самопроверяемости структуры используется перебор вариантов доопределения функций дополнения. Таких вариантов имеется большое количество.

Результатами настоящего исследования предложен способ формализации процедуры доопределения значений функций логического дополнения, основанный на учете ограничений на полностью самопроверяемые структуры систем функционального контроля. Для системы на основе метода логического дополнения требуется подача на входы тестера и элементов сложения по модулю два блока логического дополнения всех тестовых комбинаций. Предложены варианты

функций дополнения, позволяющие решать данную задачу. Каждый из вариантов будет давать разные результаты как по характеристикам обнаружения ошибок в контролируемом объекте, так и по структурной избыточности системы функционального контроля.

При построении систем функционального контроля выходы контролируемых схем разбиваются на группы по 4 выхода в каждой, а сами выходы могут варьироваться в каждой четверке и контролироваться с учетом предложенных формул дополнения.

Плеханов П.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ НА ОСНОВЕ ВОЗМОЖНОСТЕЙ БЕСПРОВОДНОЙ СВЯЗИ ПЯТОГО ПОКОЛЕНИЯ (5G)

В соответствии с нормативным определением, «интеллектуальная транспортная система» (ИТС) – это «система управления, интегрирующая современные информационные и телематические технологии и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортно-дорожным комплексом региона, конкретным транспортным средством или группой транспортных средств с целью обеспечения заданной мобильности населения, максимизации показателей использования дорожной сети, повышения безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта». В настоящее время направление ИТС активно развивается как за рубежом, так и в России на основе использования современных технологий беспроводной связи – систем сотовой связи (GSM(-R)/GPRS/EDGE, UMTS/HSPA, LTE(-R)), систем беспроводного доступа Wi-Fi (IEEE 802.11a/b/g/n/ac), а также технологии DSRC (Dedicated Short Range Communications – «специализированная связь на коротких расстояниях»: IEEE 802.11p и IEEE 1609). При этом, для железнодорожного транспорта технология DSRC является новой, поскольку изначально она разрабатывалась для организации информационного обмена на автотранспорте.

Состав задач, решаемых в рамках ИТС, в целом, соответствует составу Рабочих групп (Working Group, WG) Технических комитетов (Technical Committee, TC) № 204 и 278, соответственно, Международной организации по стандартизации (International Organization for Standardization, ISO) и Европейского комитета по стандартизации (European Committee for Standardization, CEN), занятых стандартизацией ИТС (ISO/TC 204 и CEN/TC 278 «Intelligent transport systems» (ITS)).

В России в структуре Федерального агентства по техническому регулированию и метрологии (Росстандарте) также создан Технический комитет № 57 (ТК 57) «Интеллектуальные транспортные системы» (ИТС) с входящими в его состав профильными Подкомитетами (ПК). При этом, для реализации большинства задач, стоящих перед ИТС, необходимо использование современных технологий беспроводной связи.

Как известно, к «нулевому» поколению (0G) систем подвижной связи (СПС) относятся аналоговые системы, позволяющие организовать речевую связь (возможность передачи и приема данных отсутствует) в одном из двух режимов: одночастотном симплексном и полудуплексном (двухчастотном симплексном). К первому поколению (1G) относятся аналоговые СПС, позволяющие организовать речевую связь (возможность передачи и приема данных также отсутствует) в дуплексном режиме. Ко второму поколению (2G) относятся цифровые СПС, позволяющие организовать передачу и прием речи и данных как в режиме коммутации каналов, так и в режиме коммутации пакетов. Наиболее распространенной СПС второго поколения является система сотовой связи стандарта GSM(-R)/GPRS/EDGE. СПС третьего (3G) и четвертого (4G) поколений предоставляют возможность подвижным абонентам передавать данные со скоростями, равными десяткам и сотням Мбит/с. Наиболее распространенным представителем третьего поколения СПС является технология UMTS/HSPA. Представителями четвертого поколения СПС, скорость передачи данных в которых может достигать нескольких сотен Мбит/с, являются технологии WiMAX (IEEE 802.16d/e) и LTE(-R).

Что касается СПС пятого поколения (5G), то в настоящее время нет какого-либо определенного стандарта, однозначно претендующего на то, чтобы быть представителем пятого поколения. Однако, функциональные требования к СПС пятого поколения сегодня, в целом, сформулированы и заключаются в следующем:

- значительное (в несколько раз) увеличение скорости передачи данных по сравнению со стандартами четвертого поколения;
- обеспечение доступа в сеть Интернет в любой точке со скоростью не менее 1 Гбит/с;
- переход на «облачную» инфраструктуру, использование масштабируемой и экономичной транспортной сети;
- обеспечение гарантированного уровня качества для любых видов услуг (QoS).

Очевидно, что возможности СПС пятого поколения могут быть в полной мере использованы как на обычном, так и на высокоскоростном железнодорожном транспорте при реализации концепции ИТС – например, для управления движением поездов при помощи подвижных блок-участков. При этом, необходимо учитывать все возможные риски, связанные с обеспечением безопасности движения.

Правдухина А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

СИСТЕМЫ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ НА ОСНОВЕ КОДОВ С СУММИРОВАНИЕМ С ОДНИМ ВЗВЕШЕННЫМ РАЗРЯДОМ

При построении надежных устройств автоматики часто используют системы с обнаружением неисправностей – системы функционального (рабочего) контроля. В их основе лежит заранее выбранный помехоустойчивый код с небольшой избыточностью. В системе функционального контроля важно оперативно идентифицировать возникшую неисправность, а также отключить рабочие выходы от объектов управления. По этой причине при синтезе систем функционального контроля применяют коды с обнаружением ошибок – они имеют меньшую избыточность, чем коды с корректированием ошибок.

Выбранный на этапе проектирования системы функционального контроля код однозначно определяет ее ключевые характеристики: структурную избыточность, свойства обнаружения ошибок контролепригодность и др.

При построении систем функционального контроля используются классические, модульные и модифицированные коды с суммированием, имеющие различные характеристики обнаружения ошибок в информационных векторах. Значения рабочих выходов объекта диагностирования отождествляются с информационным вектором длины m, а значения выходов блока контрольной логики – с контрольным вектором длины k. Соответствие между информационными и контрольными векторами устанавливается тестером.

Недостатком классических и модульных кодов с суммированием единичных разрядов является высокий процент необнаруживаемых ошибок, особенно, в области малой кратности. Поэтому актуальным является вопрос разработки и исследования кодов с улучшенными характеристиками обнаружения ошибок в системах функционального контроля. Один из эффективных способов кодов с «хорошими» характеристиками обнаружения ошибок и невысокой избыточностью может быть получен по следующим правилам:

1. Одному из разрядов в информационном векторе приписывается весовой коэффициент *w* – некоторое натуральное число, а всем остальным – коэффициенты, равные единице.
2. Подсчитывается суммарный вес единичных разрядов в информационном векторе (вес информационного вектора *И*).
3. Число *И* представляется в двоичном виде и записывается в разряды контрольного вектора.

Исследования показали, что такой, достаточно простой, способ построения кода позволяет сохранить основное свойство классического кода с суммированием (кода Бергера) – возможность обнаружения любых монотонных искажений в информационных векторах. Это свойство лежит в основе алгоритмов построения систем функционального контроля со 100%-ным обнаружением одиночных неисправностей.

Установлено, что значение весового коэффициента взвешенного информационного разряда может быть выбрано из множества w є {1;2;…;m}. В случаях w=m, m+1, … все коды имеют одинаковые распределения необнаруживаемых ошибок по видам и кратностям.

Взвешивание одного разряда позволяет увеличить количество обнаруживаемых ошибок по сравнению с классическим кодом Бергера. При изменении значения весового коэффициента взвешенного информационного разряда в пределах 1≤w≤m получаются коды с суммированием с различными характеристиками обнаружения ошибок в информационных векторах.

С увеличением значения весового коэффициента при постоянной длине информационного вектора общее количество необнаруживаемых ошибок уменьшается и достигает минимального значения при w=m. При этом взвешенные коды при постоянной длине информационного вектора имеют постоянное количество симметричных необнаруживаемых ошибок, а с увеличением значения взвешенного коэффициента уменьшается количество асимметричных ошибок.

В работе был поставлен ряд экспериментов по синтезу систем функционального контроля на основе взвешенных кодов с суммированием на контрольных комбинационных схемах LGSynth`89.

В эксперименте подтверждаются теоретические исследования свойств кодов. Отдельным результатом работы является анализ структурной избыточности систем функционального контроля на основе взвешенных кодов с суммированием.

Для ряда комбинационных схем подбором взвешиваемого разряда удается достичь 100%-ного обнаружения одиночных неисправностей с небольшими аппаратурными затратами.

Приходько А.М., Приходько В.М.
Украина, г. Днепр, Национальная металлургическая академия Украины
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МЕТОДЫ ПОВЫШЕНИЯ ПОКАЗАТЕЛЕЙ РАБОТЫ ДВИГАТЕЛЕЙ НА ВОДНОМ ТРАНСПОРТЕ

В связи с возрастанием цен на энергоносители и ограниченными возможностями увеличения мощности судовых энергогенерирующих установок проблема энергосбережения, в том числе снижения энергопотребления в отрасли водного транспорта, приобретает особую актуальность. Известно, что вопросы автоматизации судовых технологических процессов на водном транспорте следует решать при условии рационального соотношения между уровнем автоматизации и технологии с учётом требований к качеству процесса управления. Учитывая то, что среди судовых электроэнергетических установок доминирующее положение занимают автоматизированные дизель – генераторные агрегаты, их массовое применение на морском и речном транспорте позволяет решать не только технологические задачи, но и проблему энергосбережения. Эффективность проводимых мероприятий по ресурсо – и энергосбережению на водном транспорте достигается при обязательном применении средств комплексной автоматизации. Радикальным способом повышения КПД поршневых ДВС может стать нетрадиционная организация осуществления рабочих циклов, а именно переход на замкнутый цикл с искусственным рабочим телом на основе одноатомных (инертных) газов, значение k которых имеет наибольшую величину среди газообразных химических элементов, а теплоемкость мало меняется с изменением температуры. Применительно к различным транспортным и технологическим машинам поиск систем и средств, обеспечивающих работоспособность энергетических установок вне зависимости от атмосферного воздуха является актуальной проблемой с точки зрения решения вопроса их эксплуатации в условиях аномального состояния атмосферы. Сравнение циклов по КПД для различных значений не может быть выполнено известными способами, привлекающими диаграмму T-S (температура – энтропия), а из-за указанного выше изменения k по мере совершения цикла нельзя выполнить корректное сравнение и по формулам для термического КПД.

Целью расчетного исследования являлось выявление связи между выходными параметрами двигателя и составом рабочего тела для ДВС замкнутого цикла с углеводородным горючим и выявление оптимального состава рабочего тела. В ДВС разомкнутого цикла горючая смесь состоит из трех компонентов: горючее + O2 + балласт, а в качестве балласта выступает N2 атмосферного воздуха. Для замкнутого цикла с газообразным горючим применима схема со смесью из 2-х компонентов при рециркуляции одного из компонентов, выполняющего роль балласта. Балластный компонент рабочего тела, исходя из вышеизложенных соображений, должен быть инертным одноатомным газом с как можно меньшим изменением теплоемкости при изменении температуры. При выборе его должны учитываться также требования малой стоимости и недефицитности. Такими компонентами могут быть гелий и аргон, широко используемые в технике, причем концентрация аргона в воздухе составляет 0,93 % и его получение из воздуха налажено. Моделирование рабочих процессов ДВС выполнено на ПЭВМ по усовершенствованной расчетной методике, основа которой – стационарная термодинамическая модель Гриневецкого – Мазинга, принимающая во внимание особенности действительного цикла. Расчеты выполнены применительно к двигателю внешнего смесеобразования без наддува 4Ч 8 / 7,6 с эффективной мощностью Ne = 56,8 кВт при частоте вращения n = 5600 об / мин и параметрах на впуске P0 = 0,1 МПа, T0 = 298 К, по которому имеются полные данные о действительном рабочем цикле и дизельному двигателю без наддува Ч 26/26 с такими параметрами: диаметр рабочего цилиндра D = 26 см; ход поршня S = 26 см; частота вращения коленчатого вала n = 1000 об/мин; степень сжатия ε = 13,5; коэффициент избытка кислорода для горения дизельного топлива α = 1,8 при цикловой подаче топлива qц = 0,5637 г/цикл; коэффициент остаточных газов 0,035; коэффициенты использования теплоты к концу видимого горения 0,76 и к концу расширения 0,9; механический КПД двигателя 0,8; параметры свежей смеси перед впускными органами стандартны. Результаты расчетов показали повышение эффективного КПД ДВС при использовании Ar или He на 23 %. По результатам расчетов найдена неочевидная закономерность расположения вида балластных газов в ряд CO2, H2O (пар), O2, N2, Ar, He в соответствии с уменьшением их мольной теплоемкости по мере роста эффективного КПД соответственно 0,2234; 0,2627; 0,2998; 0,3109; 0,4015; 0,4036. Если оценить дополнительные потери в 5 %, то рост эффективного КПД ДВС с аргоновой газовой смесью, в сравнении с воздушным разомкнутым циклом, составит 17 %. Выводы: балластные компоненты рабочего тела поршневых ДВС по мере роста КПД цикла располагаются в ряд с уменьшением величины их мольных теплоемкостей; исходя из экономичности цикла ДВС и доступности наилучшим балластным компонентом рабочего тела является аргон; для ДВС, работающего на жидком углеводородном топливе, переход на замкнутый цикл с воздухоподобной смесью на аргоне может дать повышение КПД на 17 % при некотором росте показателей цикла, характеризующих тепловую и механическую напряженность деталей двигателя.

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АСИНХРОННЫХ ДВИГАТЕЛЕЙ ДЛЯ СУШКИ ИЗОЛЯЦИОННЫХ СИСТЕМ НА ВОДНОМ ТРАНСПОРТЕ

В соответствии с Федеральным Законом № 261 – ФЗ «Об энергосбережении и о повышении энергетической эффективности…» от 23 ноября 2009 г., а также с постановлением правительства Санкт – Петербурга № 1257 от 11.11.09 г. «О повышении энергетической эффективности и энергосбережении» разработка эффективных методов, средств контрольного прогрева, подсушки, сушки, восстановления изоляционных систем, диагностики и интенсификации комплексных испытаний электрооборудования судов по энергосберегающей технологии в судостроении и судоремонте является для морского и речного флота актуальной проблемой.

В электроцехах судостроительно – судоремонтных предприятий и на судах речного, морского, рыбопромыслового флотов в судовых эксплуатационных условиях качество перемотки статорных обмоток в технологическом процессе ремонта судовых асинхронных двигателей (АД) можно оценить при нагреве неподвижных электродвигателей, когда в обмотки статоров подаётся постоянный ток, управляемый с помощью разработанных портативных универсальных тиристорных преобразователей. Приведены экспериментальные и расчетные данные для АД типа 4АХ90L4У3 номинальной мощностью, равной 2,2 кВт. Экспериментальные и расчетные данные с достаточной точностью совпадают. Однако, необходима дальнейшая корректировка методики расчета с учетом экспериментальных данных, так как тепловые связи между статорной обмоткой и пакетом частей статора зависят от качества пропитки обмоток, которая может быть разной. Поэтому необходимо проводить дальнейшие исследования, чтобы уточнить достоверность характера процесса нагрева исправной обмотки. Показаны кривые нагрева обмоток статора судового АД постоянным током, регулируемым разработанным тиристорным преобразователем, в сравнении с опытными и расчетными данными, где видно, что точность расчетов для бóльших токов ниже. Однако выражение после соответствующей корректировки по опытным данным может служить основой для управления процессом нагрева АД в режиме прогрева, подсушки, сушки с помощью микропроцессора с учетом допустимой погрешности. В связи с тем, что за основу принят способ сушки постоянным током, то было проведено исследование электрических характеристик обмоток судовых асинхронных двигателей, получивших наибольшее распространение в отрасли водного транспорта. Представлены экспериментальные характеристики нагрева обмоток статоров судовых асинхронных двигателей новой серии 4А номинальной мощностью 1,1 и 2,2 кВт, как в собранном виде, так и только одного статора, при пропускании через обмотки постоянного тока различного значения, управляемого разработанным тиристорным преобразователем переносного типа. Получена серия графиков нагрева судовых асинхронных двигателей различной мощности токами, величина которых регулируется с помощью переносного тиристорного преобразователя. При разработке способа и устройств ускоренной энергосберегающей сушки изоляции увлажненных обмоток в процессе экспериментальных исследований решен ряд задач: определено температурное поле АД; определена предельно допустимая величина тока при форсированном режиме; определены величины напряжения, активной мощности, времени и расхода электрической энергии при сушке.

Проведённые исследования также могут найти применение в отрасли водного транспорта для широкого круга задач по определению температуры твердых сред, находящихся в непосредственном тепловом контакте.

Приходько В.М., Приходько И.В., Лучкин В.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

АВТОМАТИЗАЦИЯ ОПРЕДЕЛЕНИЯ ТОКОВ АВАРИЙНЫХ ДУГОВЫХ КОРОТКИХ ЗАМЫКАНИЙ НА ВОДНОМ ТРАНСПОРТЕ

Выполнены автоматизированные расчеты токов короткого замыкания (КЗ) с учетом сопротивления электрической дуги для мощных судовых электроэнергетических систем (СЭЭС) с номинальными напряжениями 0,22; 0,38 и 0,5 кВ. При расчетах на компьютере учитывались сопротивления кабелей, шин, трансформаторов тока, автоматических выключателей, а также активные сопротивления судовых генераторов, питающих места КЗ. Выбор уставок защит производился на основании результатов расчетов токов КЗ с учетом сопротивления электрической дуги в момент ее возникновения. В первые периоды возникшего повреждения СЭЭС длина и сопротивление дуги имеют минимальные значения, а ток КЗ – максимальное. В последующие периоды по мере удлинения электрической дуги под влиянием конвекции воздуха и электродинамических усилий длина и сопротивление электрической дуги могут существенно возрастать. Существующая методика однократного расчета сопротивления дуги по известному выражению не всегда обеспечивает необходимую точность расчета. Точное сопротивление дуги может быть получено в результате проведения большого числа последовательных расчетов, выполнение которых необходимо осуществлять на компьютере (микрокалькуляторе) в специальной

программе. Для выполнения расчетов предложена формула, в которую вводятся суммарные сопротивления судовой сети и коэффициент А в соответствии с видом КЗ (однофазное, двухфазное или трехфазное симметричное).

Для автоматизации, упрощения и ускорения расчетов сопротивления дуги по предложенной формуле, а также суммарных сопротивлений судовой сети и токов аварийных КЗ разработана программа расчетов на компьютере (микрокалькуляторе).

Разработан алгоритм расчетов токов двухфазного и однофазного КЗ с учетом сопротивления дуги для автономных (судовых, корабельных) электроэнергетических систем. Расчет суммарных сопротивлений судовой электрической сети производился в соответствии с типовой методикой, разработанной ЦНИИСЭТ. Сопротивление электрической дуги в момент ее возникновения вычислялось по предложенной формуле. Все расчеты производились на компьютере (отечественном микрокалькуляторе) по разработанному алгоритму и реализованной рабочей программе. Анализ выполненных автоматизированных расчетов показывает, что токи КЗ с дугой в момент ее возникновения уменьшаются относительно токов КЗ без дуги до 0,835 – 0,495 при двухфазных аварийных КЗ и до 0,685 – 0,355 при однофазных. Сопротивление электрической дуги в месте аварийного КЗ существенно зависит от активного сопротивления судовой питающей сети. Значительная разница в величинах отношений при двухфазных и однофазных КЗ на различных судовых секциях 0,38 кВ определяется отличием суммарных активных сопротивлений судовой сети до соответствующих мест КЗ на судах. Определение сопротивления дуги целесообразно производить автоматизированными расчетами с учетом сопротивлений всех элементов электрической сети судна.

При автоматизированном проектировании СЭЭС использование в расчетах токов КЗ только заданных определенных сопротивлений дуги или коэффициентов запаса в случае выбора уставок защит без учета реальных сопротивлений судовой сети и расчетных сопротивлений электрической дуги в месте КЗ приводит часто к завышению токов КЗ и уставок быстродействующих защит, а иногда и к их занижению.

Зависимость токов КЗ от длины дуги в относительных единицах при автоматизированных расчетах без учета активного сопротивления судовой сети одинакова для СЭЭС любого напряжения. Обычно в расчетах токов КЗ на компьютере не учитываются активные сопротивления высоковольтных судовых сетей из-за их малой величины. Значительное уменьшение аварийных токов КЗ в зависимости от длины электрической дуги определяется наличием активного сопротивления судовой сети. Увеличение длины и сопротивления электрической дуги в процессе КЗ может привести к ее погасанию на судах.

В СЭЭС 0,38 кВ при расстоянии между токоведущими частями в месте КЗ 0,15 м электрическая дуга может погаснуть после ее возникновения при двухфазном КЗ через 0,24 – 0,4 с, а при однофазном – через 0,14 – 0,28 с. В действительности электрическая дуга погаснет при меньшей ее длине, чем максимальная, что приведет к уменьшению расчетного времени горения дуги в СЭЭС. Установлено, что через небольшой промежуток времени после погасания электрическая дуга загорится вновь при минимальной ее длине. В СЭЭС возникнет процесс аварийного КЗ через прерывистую дугу. На судах защиты при аварийных КЗ через перемежающуюся дугу отказывают в действии, если время их действия больше времени горения дуги до ее погасания, так как при погасании дуги или даже несколько раньше при уменьшении тока КЗ происходит возврат токовых реле и сброс набранной выдержки времени защиты. Это подтверждается также опытом эксплуатации мощных СЭЭС.

Приходько В.М., Приходько И.В., Игнатов Д.И.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ИНФОРМАЦИОННЫЙ АСПЕКТ ПРОБЛЕМЫ ЭНЕРГОСБЕРЕЖЕНИЯ НА ВОДНОМ ТРАНСПОРТЕ

В рыночной экономике требуется системный анализ оптимизации электротехнических комплексов «берег-судно», «берег-док», необходимы оптимальные решения в энергетических задачах проектирования и эксплуатации судовых электроэнергетических систем (СЭЭС), при автоматизированных комплексных испытаниях судовых электростанций по энергосберегающей технологии. В настоящее время необходима оценка влияния случайных факторов на функционирование объектов (систем) водного транспорта, включая суда, порты и гидротехнические сооружения. Под системностью подразумевается использование системного анализа, предполагающего следующие действия: выявление закономерностей процессов в СЭЭС, зависимости от внутренних и внешних факторов, установление взаимосвязей между факторами; учет всех факторов, влияющих на процесс; учет глобальной (конечной) цели всей СЭЭС при решении частных (промежуточных) задач; прогноз возможных последствий от принятого решения (ближайших и отдалённых). При системном подходе к проблеме энергосбережения становится очевидным, что энергосбережение не является самоцелью, а должно послужить укреплению экономики и улучшению качества жизни. Поэтому на объектах водного транспорта нельзя экономить на здоровье людей, на первоочередных социальных потребностях при замене тяжелого физического труда и на снижении

качества строящихся и ремонтируемых судов, т.е. необходимо экономить энергоресурсы любой ценой. На судах, гидротехнических сооружениях, судоремонтно-судостроительных предприятиях, в морских и речных портах, а также при создании электротехнических комплексов «берег-судно», «берег-док» и всесторонних испытаниях автоматизированных судовых электростанций по ресурсоэнергосберегающей технологии с отдачей электроэнергии в береговую сеть бесконечной мощности. В современной экономике проблема энергосбережения, повышенное внимание к которой характерно для трех последних десятилетий как во всем мире, так и в нашей стране, имеет много аспектов. В отличие от часто обсуждаемых технических и технологических вопросов энергосбережения и ресурсосбережения рассмотрим тот аспект проблемы, который условно можно назвать «информационным». Информационные технологии, связанные, прежде всего с использованием современной компьютерной техники и средств сбора и передачи данных, открывают новые возможности при решении вопросов ресурсо- и энергосбережения. Если компьютеризация решения задач оптимизации технологических процессов (например, наладка тепловой сети), минимизации электрических потерь, оптимизация электротехнических комплексов «берег-судно», «берег-док», автоматизация испытаний судовых электростанций по энергосберегающей технологии и др. очевидно связана с экономией энергетических ресурсов, то связь с энергосбережением других задач, решаемых в процессе компьютеризации предприятий энергоснабжения объектов водного транспорта не столь очевидна. Значительным энергосберегающим эффектом обладает компьютеризация расчетов с потребителями энергии, которая связана с дисциплинирующим фактором, сопровождающим взаимоотношения поставщика и потребителя в процессе компьютеризации учета. В современных экономических условиях использование компьютеров освобождает сотрудников энергосберегающих предприятий от значительной доли рутинного труда, связанного с проведением расчетов оплаты отпущенной энергии, подготовки платежных документов, учета проведенных оплат, должников и др. Компьютеризация расчетов с потребителями, в том числе морской и речной транспорт, открывает практическую возможность к переходу на новые, современные формы расчетов, такие как использование предварительной оплаты, проведение гибкой тарифной политики и др. Для отрасли водного транспорта важно, что компьютеризация, а особенно офисная компьютеризация, среди всех направлений энергосбережения имеет наилучшее соотношение «результат/цена». В отличие от других направлений, компьютеризация не требует значительных материальных вложений, а имеющиеся в настоящий момент невысокие цены на средства вычислительной техники и соответствующее программное обеспечение (ПО) позволяют развивать это направление практически всем энергоснабжающим предприятиям. Немаловажным фактором является и то, что использование современных информационных технологий существенно меняет характер труда работников абонентских отделов, ПТО и бухгалтерий предприятий, делает его более привлекательным, что в свою очередь обеспечивает приход в эту сферу деятельности более квалифицированных кадров. В России уже накоплен значительный опыт эксплуатации отечественного программного обеспечения, обслуживающего информационные процессы на тепло- и элетроснабжающих предприятиях. Руководители и специалисты предприятий могут выбрать не только подходящее ПО, но и познакомиться с опытом его эксплуатации на аналитических предприятиях, включая судостроительно-судоремонтные, оценить удобство работы, качество поддержки разработчиком пользователей. Важность компьютеризации как энергосберегающего фактора еще не оценена в полной мере. Целесообразно, чтобы отраслевые структуры морского и речного транспорта, а также многочисленные общероссийские и региональные центры энергоснабжения обратили внимание на эту проблему.

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ТЕХНИКО-ЭКОНОМИЧЕСКИЙ АНАЛИЗ СУДОВЫХ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ С ПОЛУПРОВОДНИКОВЫМИ ПРЕОБРАЗОВАТЕЛЯМИ

На водном транспорте автоматизированные судовые электроэнергетические системы (СЭЭС), содержащие мощные полупроводниковые преобразователи, характеризуются резкопеременными, импульсными, несимметричными и несинусоидальными режимами работы, вызывающими отклонения показателей качества электрической энергии (ПКЭ) от нормативов, установленных Морским регистром судоходства РФ и Российским речным регистром. Ухудшение качества электроэнергии отрицательно сказывается на работе других судовых потребителей. На судах снижается надежность электроснабжения, электро- и пожаробезопасность, увеличиваются потери электроэнергии, повышается вероятность выхода из строя или отказов отдельных типов судового электрооборудования, электронного оборудования, систем управления, телемеханики и связи, информационно-измерительных систем. Наличие в СЭЭС резкопеременных и несинусоидальных нагрузок усложняет задачи компенсации перетоков электроэнергии и обменных процессов, поскольку традиционные способы компенсации не всегда приемлемы на судах. Улучшение показателей качества электрической энергии, оптимизация энергопотребления в нелинейных системах

электроснабжения на судах за счет приемлемых технических решений СЭЭС требует комплексного технико-экономического анализа.

Исходными данными для технико-экономического анализа являются структура и состав СЭЭС, характеристики, отражающие качество электроэнергии и процессы энергообмена в ней. Для действующей эксплуатируемой СЭЭС все требуемые параметры определяются на основе измерений физических величин. При проектировании СЭЭС исходными данными служат результаты моделирования энергетических процессов с учетом специфики работы всех судовых потребителей.

Технико-экономический анализ СЭЭС с мощными полупроводниковыми преобразователями состоит из следующих основных этапов: количественная и качественная оценка энергопотребления и качества электрической энергии; определение экономического ущерба в системе из-за отклонений ПКЭ и неоптимального энергопотребления; выбор комплекса технических мероприятий по улучшению энергопотребления и компенсации искажений сетевого напряжения; оценке эффективности выбранного решения.

В настоящее время необходима разработка счетчиков судового исполнения, построенных на новых принципах и измеряющих обменную энергию и энергию накопления, которые позволят более полно охарактеризовать СЭЭС с точки зрения оптимальности процессов передачи и потребления электрической энергии на судах морского и речного флота. По результатам измерений ПКЭ на основе топологии и состава СЭЭС определяются причины возникновения искажений в питающей судовой сети и типы нагрузок, на которые могут оказать влияние эти искажения. Затем определяется экономический ущерб. Ущерб из-за снижения качества электроэнергии обуславливается следующими факторами: отклонениями частоты питающего судового напряжения; колебаниями частоты; отклонениями судового напряжения; колебаниями судового напряжения; несимметрией и неуравновешенностью судового напряжения (оцениваются соответственно коэффициентами несимметрии напряжения и неуравновешенности напряжения); несинусоидальности судового напряжения (характеризуется коэффициентом несинусоидальности напряжения). Величина ущерба, его причины и структура являются исходными данными при разработке технических и организационных мероприятий, направленных на повышение эффективности функционирования СЭЭС. Если ущерб обусловлен влиянием низкого качества электрической энергии на судовое электротехническое и технологическое оборудование, то технические мероприятия должны быть направлены в первую очередь на снижение этого влияния за счет улучшения качества электроэнергии. Затем уже решается задача оптимизации энергопотребления в СЭЭС, которая сводится в этом случае к компенсации реактивной составляющей тока. Если однозначное принятие решения затруднено, необходимо проработать альтернативные варианты с последующей сравнительной оценкой. Для сравнения вариантов технических решений следует располагать следующими обобщенными показателями: капитальные вложения, которые необходимы для создания технических средств; ежегодные издержки, необходимые для функционирования технических средств; потребительский эффект, выражает снижение ущерба из-за улучшения ПКЭ и параметров энергопотребления (ЭП). Технико-экономический анализ нелинейных СЭЭС с мощными полупроводниковыми преобразователями (неуправляемыми выпрямителями, управляемыми выпрямителями или тиристорными преобразователями, инверторами, полупроводниковыми преобразователями частоты, тиристорными преобразователями постоянного напряжения) позволяет принять наиболее оптимальное решение по улучшению энергопотребления и качества электрической энергии на судах. Сложность проводимых аналитических расчетов, значительный объем необходимой информации требуют разработки алгоритмических средств технико-экономического анализа, создания банка данных, обладающего требуемой информационной полнотой.

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

КРИТЕРИЙ ОЦЕНКИ ПОТЕРЬ ПРИ РАСПРЕДЕЛЕНИИ ЭЛЕКТРОЭНЕРГИИ В СУДОВЫХ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМАХ

На водном транспорте совокупность мер, направленных на снижение потерь при распределении электроэнергии включает в себя, как одну из составляющих, уменьшение действующего значения тока в кабельной линии при тех же значениях напряжения судового синхронного генератора. В синусоидальных цепях эта задача решается однозначно, посредством компенсации реактивной мощности судовых потребителей электроэнергии. Для несинусоидальных судовых цепей единого подхода к компенсации реактивной мощности не имеется. Это связано с наличием для таких цепей известного множества определений реактивной мощности. Часто при введении определений оставлялась без внимания зависимость величины реактивной мощности от действующего значения тока. Показана зависимость для наиболее распространенных определений реактивной мощности. Рассмотрена судовая электроэнергетическая система (СЭЭС), состоящая из генератора напряжения и подключенной к нему нагрузки с током. Если функции напряжения и тока

квадратично интегрируемы на интервале времени, то для них выполняется неравенство Коши-Шварца.

Из полученного неравенства следует, что передача в нагрузку активной мощности может происходить при различных значениях действующего тока. Величина действующего значения тока будет минимальна (для данных активной мощности и напряжения судового генератора), если активная мощность равна полной мощности. Степень отклонения активной мощности от полной характеризуется с помощью реактивной мощности Фризе. Неравенство превращается в тождество (условие равенства нулю реактивной мощности Фризе) только в том случае, когда функции напряжения и тока линейно зависимы, при этом в судовую нагрузку будет передаваться активная мощность, если коэффициент пропорциональности между ними равен отношению активной мощности к квадрату напряжения генератора судовой электростанции.

Из предложенного выражения следует, что на водном транспорте компенсация реактивной мощности Фризе аналогична минимизации действующего значения тока, протекающего от судового генератора к нагрузке. На судах минимизация осуществляется посредством подключения параллельно судовой нагрузке компенсатора с током равным по величине, но противоположным по направлению. Преобразование энергии в судовой нагрузке определяется с помощью скалярного произведения функций напряжения и тока, которое не отражает наличие в составе тока его реактивной составляющей. Ортогонализация одной из функций в произведении напряжения и тока во многих случаях приводит к возможности учета реактивной составляющей тока. На основании такого подхода представлено определение следующих реактивных мощностей: I) интегральной реактивной мощности по Будеану; 2) мощности с использованием значения производной по времени от одной из определяющих функций напряжения или тока; 3) мощности с применением значений интеграла по времени от одной из определяющих функций напряжения или тока. Даны существенные недостатки для вышеперечисленных определений реактивной мощности.

Установлено, что причиной недостатков является то, что суммирование в известных аналитических выражениях происходит с учетом знака реактивной мощности к-ой гармоники.

Возможность разделения тока нагрузки на составляющие, а, следовательно, возникновение дополнительных потерь при передаче энергии на водном транспорте может быть связано с наличием в цепи накопителей электромагнитной энергии, ключевых элементов, нелинейностей – как реактивных, так и активных.

Одной из характеристик, отражающих накопление электромагнитной энергии в цепи и обмен энергией между судовым генератором и нагрузкой является обменная мощность, которая определяется как мощность, запасенная в реактивных элементах цепи за определенный интервал времени, в течение которого мгновенная активная мощность больше нуля.

Обменная мощность также не может служить для оценки дополнительных потерь при передаче энергии от судового генератора к нагрузке, так как отражает только одну сторону возникновения этих потерь – наличие в цепи реактивных элементов. Ей присущи те же недостатки, что и мощностям: по Будеану; с использованием значения производной по времени от одной из определяющих функций напряжения или тока; с применением значений интеграла по времени от одной из определяющих функций напряжения или тока.

Наиболее наглядно это видно из анализа соотношения между обменной и мощностью Фризе для битиристорного регулятора с активной нагрузкой и углом открывания тиристоров, подключенного к синусоидальной ЭДС (снижение действующего значения тока за счет компенсации реактивной мощности первой гармоники влечет за собой появление обменной мощности).

Следовательно, реактивная мощность Фризе является наиболее полной из рассмотренных определений реактивных мощностей характеристикой энергетических процессов в СЭЭС с точки зрения эффективности передачи электроэнергии на судах морского и речного флота.

Ревера Г.М.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

СТЕГАНОГРАФИЯ НА ВОДНОМ ТРАНСПОРТЕ

Морские перевозки не одно столетие являются одним из самых эффективных способов грузового сообщения. Для их успешной реализации морякам необходимо получать множество информации, в частности навигационные и метеорологические предупреждения, метеорологические прогнозы и другие срочные сообщения, относящиеся к безопасности.

Сама по себе передача информации не составляет труда, для этого существует множество возможностей как физической передачи, так и через вычислительные сети. Но порой бывает необходимо передать информацию непредназначенную для посторонних или даже совершенно конфиденциальную. Один из способов использовать шифрование, но и этот метод бывает ненадежен, ведь любой шифр можно взломать, а вот если воспользоваться стеганографией и сокрыть сам факт передачи документа, то есть шанс в успешной передаче данных. Выгоднее всего использовать стеганографию.

Стеганография – это наука о сокрытой передачи данных путем сохранения самого факта передачи данных. Сама наука появилась очень давно, но вот ее раздел – цифровая стеганография появилась сравнительно недавно - во времена развития информационных технологий. Но и тут все может пойти не так гладко, как нам кажется. Для того чтобы передать необходимую информацию необходимо поместить ее в пустой контейнер, для этого используют одну из программ, предоставленную на рынке IT технологий. Сложность состоит в том, что получатель данной информации должен знать: во-первых – программу, которой воспользовался отправитель, во-вторых – знать о самом факте передачи. Иначе, пользуясь другой программой для расшифровки сокрытой информации получатель имеет все шансы повредить или даже уничтожить ее. А не зная, что факт отправки информации был совершен вообще может пропустить ее. Поэтому логично заранее подобрать программу для стеганографической передачи, ведь от выбора программы зависит какой из алгоритмов будет использоваться при сокрытии данных. А также необходимо продумать о том, когда следует ждать самого факта передачи. Для этого целесообразно отправителю и получателю заранее обдумать этот вопрос, ведь может возникнуть ситуация, когда получатель не сможет узнать о свершенной передачи, потому что находился в море вне систем связи.

Седых Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

МЕТОДЫ СВЕРКИ ЧЕРТЕЖЕЙ НАПОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

В настоящее время все проектные организации в сфере железнодорожного транспорта перешли на выполнение проектирования в электронном виде с помощью компьютерного программного обеспечения. Но является ли такое проектирование реальным отличием от проектирования на бумаге? Для многих операций программные средства систем автоматизированного проектирования (САПР) используются только как инструмент рисования, где реализуются функции карандаша и линейки на компьютерном экране с помощью мыши.

САПР является инструментом или средством, позволяющим повысить качество и сократить сроки выполнения проектов за счет автоматизации различных проектных операций и выявления некоторых технических ошибок, допускаемых во время проектирования

Процесс проектирования является комплексным и должен предусматривать единую модель данных для всех составляющих проекта, так как они очень зависимы между собой. Только построение единой модели может дать возможность контроля выполнения отдельных разделов и их увязки с другими разделами проекта.

Основной составляющей проекта по железнодорожной автоматике и телемеханики (ЖАТ) являются чертежи, выполняемые в стадии проектной документации. В него входят следующие виды чертежей: схематический план станции, таблица взаимозависимостей стрелок, сигналов и маршрутов, двухниточный план станции, схема канализации тягового тока, схема кабельной сети.

Отдельной сложной процедурой проектирования можно выделить внесение изменений в отдельные документы проекта. Применительно к данной операции можно говорить про «внесение изменений в процессе выполнения нового проекта», а также «в процессе внесения незначительных изменений в действующий проект». Изменения, закладываемые в один из чертежей, требуют обязательного внесения изменений в другом. Не всегда внесение изменений в другой чертеж можно сделать автоматически без участия человека, но программное обеспечение может отследить и проконтролировать внесение изменений во все чертежи проекта и помочь пользователю проконтролировать изменение технической документации.

Для построения единого представления документации был разработан отраслевой формат технической документации на устройства ЖАТ (ОФ-ТД СЦБ), способный представить всю необходимую документацию на них. ОФ-ТД СЦБ содержит в себе не только информацию об изображении чертежа (в универсальном формате векторной графики – Scalable Vector Graphics (SVG)), но и модель изображенного на ней элемента или схемы. При этом приложение может извлекать необходимую информацию по требованию (только графику, или только модель, или и то и другое). Также чертеж в ОФ-ТД СЦБ может быть прочитан не только специализированным приложением, но и обычным браузером. В настоящее время ОФ-ТД СЦБ уже используется для обмена информацией как между различными программными системами, так и как формат обмена внутри отдельных программных продуктов.

Отраслевой формат технической документации позволяет описать все виды чертежей напольного технологического оборудования как модель, что позволяет на базе данного формата построить модули контроля внесения изменений в любой из чертежей.

Актуальной задачей при проверке и экспертизе технической документации является сверка технической документации друг с другом. Это актуально для ряда чертежей, получаемых в результате сквозного проектирования друг из друга. Например, схематический план станции является

первичной схемой при любом проектировании устройств автоматики. На его основе строится двухниточный план станции и далее – схема канализации тягового тока. Все эти чертежи строятся друг из друга и содержат новые подмножества параметров и дополнительных элементов по сравнению с предыдущим чертежом. Все данные схемы (их основа) представляют собой связанные графы, где вершинами графа являются основные элементы топологического развития, а ребрами графа – участки путей (рельсы). В общем случае задача сравнения таких схем сводится к идентификации вершин графа на соответствие и сравнению графов между собой.

Использование описания рельсовых цепей в отраслевом формате с разработанной структурой позволило значительно упростить задачу сверки. Теперь схему можно представить графом меньшей размерности, где вершинами являются рельсовые цепи, а ребрами графа – связи между границами рельсовой цепи. Данное представление позволило не только использовать второй раз многие алгоритмы «как есть», но и сократить время работы алгоритма в несколько раз.

Проведенный опыт по разработке системы экспертизы показал, что применение данного формата и описаний рельсовых цепей для схем напольного технологического оборудования ЖАТ позволяет упростить разработку модулей сверки технической документации.

Тришин Н.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ДОСТИЖЕНИЕ ОПТИМУМА РЕДУКЦИИ КОНЕЧНОГО АВТОМАТА С ТОЧКИ ЗРЕНИЯ ЭВРИСТИЧЕСКОГО ПОДХОДА АЛГОРИТМА STAMINA

В системах железнодорожной автоматики и телемеханики наибольшее распространение получили элементы, характеризующиеся только двумя состояниями. Построенные на них однотактные и многотактные схемы работают по законам двузначной логики, в связи с чем их называют логическими устройствами.

В многотактных схемах процесс преобразования входной информации осуществляется значительно сложнее, чем в комбинационных. Эта сложность обусловлена тем, что всякий многотактный автомат содержит запоминающие элементы, которые в определенные моменты времени, называемые тактами, меняют свои состояния с приходом входных сигналов и совместно с ними участвуют в преобразовании информации. Все реальные многотактные автоматы имеют ограниченную память и соответственно ограниченное число внутренних состояний, поэтому многотактные автоматы называют также конечными автоматами.

Конечные автоматы или автоматы с конечным числом состояний представляют собой широкий класс устройств различных сложности и назначения – от сложнейших ЭВМ до простейших релейных устройств типа пусковой кнопки.

Важную роль играют не просто логические схемы, обеспечивающие нужное поведение, эквивалентное поведению исходного описания проектируемой цифровой системы, а схемы, оптимизированные по тем или иным критериям: стоимости, площади, быстродействию, мощности или их комбинации.

Большое значение при проектировании конечных автоматов имеет задача минимизации числа внутренних состояний автоматов с целью сокращения формы их записи и построения на минимальном количестве элементов памяти. Очевидно, сложность, а вместе с тем и стоимость автомата, не считая затраты на его проектирование, определяются числом и стоимостью всех технических элементов, составляющих его схемы. В связи с масштабностью данной проблемы речь о точных решениях, по существу, не идет – на практике используются эвристические алгоритмы, позволяющие решать задачи огромной размерности, когда число логических элементов исчисляется миллионами.

Для уменьшения степени влияния человеческого фактора и повышения надежности была создана система SIS (Sequential Interactive System) оптимизации и синтеза последовательностных схем – это классический пример исследовательского пакета программ в области логического проектирования. Данная система представляет собой набор свободно распространяемых программ, которые оперируют с различными представлениями логических схем, систем булевых функций и конечных автоматов. С целью сокращения количества состояний конечного автомата используется программа STAMINA, алгоритм минимизации которой основан на методе Грасселли и Луччио. В программе используются следующие эвристические приемы: поиск эквивалентных состояний и их последующее объединение по максимальной совместимости.

В результате знакомства с пакетом программ SIS перед автором стояла задача – доказать эффективность эвристик, используемых в алгоритме STAMINA минимизации количества внутренних состояний конечного автомата. Для обеспечения решения поставленной задачи в данной работе:

– впервые пошагово рассмотрен алгоритм STAMINA минимизации количества внутренних состояний конечного автомата в качестве эвристического алгоритма, основанного на операции объединения совместимых строк по столбцам таблицы переходов многотактной схемы;

– показан оптимальный по сравнению с алгоритмом минимизации, основанным на методе Грасселли и Луччио, подход решения задачи минимизации алгоритмом STAMINA на примере частично определенного автомата;

– затрагивается вопрос о критериях минимальности.

Стоит отметить, что подробное рассмотрение алгоритма STAMINA на русском языке не публиковалось.

Материал проделанной работы может быть применен в решении проблемы минимизации конечного автомата с целью не только сокращения формы его записи, но и получения оптимального решения в процессе его технической реализации.

Удалов В.С., Гаскаров В.Д
Россия, Санкт-Петербург, ФБУ «Администрация «Волго-Балт»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ПОЛОЖЕНИЯ СУДНА В КАМЕРЕ ШЛЮЗА ПРИ ПОМОЩИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ЗА ПРОЦЕССОМ СУДОПРОПУСКА

В настоящее время в рамках проекта «Разработка и реализация комплексного проекта реконструкции Волго-Балтийского водного пути» ведутся работы по замене морально устаревшего и изношенного оборудования судоходных шлюзов. В части систем управления процессом судопропуска внедряются автоматизированные системы управления судопропуском на шлюзах Волго-Балтийского бассейна внутренних водных путей. Одной из их подсистем является система видеонаблюдения за процессом шлюзования.

На большинстве шлюзов в процессе вхождения судна в камеру шлюза и остановки в ней для ошвартовывания за положением судна в камере шлюза наблюдает судопропускник и старший диспетчер-начальник вахты. Делается это для того, чтобы судно в процессе шлюзования не повредило важные элементы гидросооружения и не нарушило целостность обшивки и агрегатов в процессе наполнения или опорожнения камеры. Кроме того наблюдение за положением судов в шлюзовой камере необходимо, чтобы судно не создавало помех при створении основных двустворчатых ворот или при подъеме основных подъемно-опускных ворот. В процессе модернизации систем управления судопропуском применяются современные оптоэлектронные устройства, работающие по принципу «прерывание луча», но это может быть неэффективно при плохой видимости или загрязнении приемопередающего устройства, поэтому без помощи судопропускника диспетчеру сложно обходиться.

На шлюзах повсеместно установлены или устанавливаются системы видеонаблюдения, которые используются только по прямому своему назначению – для обеспечения возможности удаленно просматривать и обеспечивать возможность записи видеоинформации о процессе шлюзования. Однако, одна возможность использования систем видеонаблюдения, а именно обеспечение правильного положения судна в камере шлюза путем определения движущихся объектов в секторе обзора видеокамер, не используется. Исправив эту ситуацию можно обеспечить значительно более высокий уровень безопасности в процессе шлюзования как для судна,так и для самого шлюза.

Автоматизированные системы управления процессом судопропуска исполнены как функциональные модули, построенные на базе программируемых логических контроллеров. Когда судно будет входить в зону повышенной опасности, которая находится в секторе обзора видеокамер, от модуля системы видеонаблюдения будет отправляться сигнал на программируемый логический контроллер системы управления процессом судопропуска и отображаться в текстовой или графической форме на центральном пульте управления. Диспетчер-начальник вахты получит возможность оперативно, без помощи третьих лиц, определить насколько безопасно расположено судно в камере и дать команду судоводителю на корректировку положения.

Кроме того при помощи незначительной доработки программных средств можно с достаточно высокой точностью определять положения судов в камере шлюза относительно друг друга в случае, когда в процессе шлюзования участвует более одного судна.

Благодаря тому, что весь процесс шлюзования записывается на сервере системы видеонаблюдения, при возникновении нештатных ситуаций появится возможность по журналам, которые ведутся в автоматизированных системах управления судопропуском и данным видеонаблюдения установить причины и детально проработать весь процесс шлюзования от начала и до конца. Это позволит повысить контроль за качеством и безопасностью шлюзования и дать возможность судопропускнику следить за исполнительными механизмами, не отвлекаясь на судно. Помимо этого при дальнейшем развитии автоматизированных систем управления такое использование системы видеонаблюдения позволит в еще большей степени автоматизировать процесс судопропуска и обеспечит более высокий уровень обеспечения транспортной безопасности при шлюзовании и снизит вероятность возникновения нештатных ситуаций, связанных с «человеческим фактором»

Удалов В.С., Гаскаров В.Д.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ СТРУКТУРЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПО ИСТЕЧЕНИИ СРОКА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ПРОИЗВОДИТЕЛЯ

В настоящее время на большинстве объектов водного транспорта используются различные виды автоматизированных систем управления. Некоторые из такого рода систем смонтированы уже достаточно давно и, вследствие выработки ресурса возникают сбои в работе автоматизированных систем, построенных на базе оборудовании, которое в данный момент снято с производства. Такое оборудование требует к себе особенного внимания. Это связано с тем, что при возникновении каких-либо неполадок или сбоев в его работе будет достаточно сложно выполнить отладку программного обеспечения или же замену отдельных элементов системы, таких как панели управления, программируемые логические контроллеры. Во многих случаях замена вообще не представляется возможной в связи с тем, что производитель не поставляет данную номенклатуру оборудования, что связано в большей степени со снятием данной продукции с производства. Замена же на аналогичное оборудование, производящееся в настоящий момент, связана со сложностями в процессе монтажа и перенастройки программной части автоматизированных систем управления.

Оборудование некоторых производителей требует различных специальных устройств для обновления программной части и возникают ситуации, когда, при некорректном использовании такого оборудования или перебоев с подачей электроэнергии, скачков напряжения или иных факторов, оборудование может выйти из строя. В таком случае необходимо провести диагностику неполадок и определить степень повреждений. Для этого зачастую необходимо использование соединительных кабелей или конверторов сигнала для передачи управляющих команд на программируемые контроллеры (ПЛК) или панели оператора (ОП). Многие из таких кабелей или преобразователей используют не применяющиеся в современной технике протоколы передачи данных или разъемы для присоединения оборудования к персональному компьютеру (ПК) для внесения изменений в проект или аппаратное программное обеспечение попросту отсутствуют на современных ноутбуках и персональных компьютерах.

В таких случаях возникает множество проблем, связанных с организацией ремонта автоматизированных систем. На рынке существуют всевозможные переходники для согласования протоколов передачи данных, однако, не всегда качество работы таких переходников обеспечивает возможность корректной работы связки «ПК-ПЛК» или «ПК-ОП».

В случае, когда в наличии у эксплуатирующей организации имеется ПК старого образца и необходимая кабельная продукция, сложность задачи по восстановлению работоспособности систем управления существенно снижается. Кроме проблемы с оборудованием и устройствами для диагностики и отладки существует проблема с кадрами на предприятии. Вновь принятый на работу персонал не владеет в достаточной мере знаниями и навыками по работе со старыми версиями программного обеспечения равно как и с диагностикой неполадок у оборудования устаревшего образца. В таком случае оперативный ремонт и последующий ввод в эксплуатации невозможен. Специалист должен изучить огромное количество документации. Зачастую нужно искать решение проблемы на всевозможных специализированных формах в сети интернет. Необходимо найти соответствующие спецификации и руководства по эксплуатации и обслуживанию имеющегося оборудования, в то время как найти их достаточно сложно.

Проблемы с оборудованием, которое уже установлено и используется в работе решить можно, несмотря на значительные сложности.

Модернизация оборудования систем автоматизации не прекращается, и в рамках проектов по реконструкции на объектах внутреннего водного транспорта устанавливаются современный средства автоматизации, которые также через пять лет, а может и меньше, устареют и с обслуживанием возникнут те же проблемы, что и с уже устаревшим оборудованием. Для того, чтобы подобных сложностей избежать эксплуатирующей организации необходимо на начальном этапе эксплуатации приобрести в резерв достаточное количество запасных элементов и необходимые средства для диагностики, обслуживания и ремонта средств автоматизации.

Кроме наличия оборудования необходимо запастись технической документацией, инструкциями по обслуживанию и ремонту имеющегося оборудования. Этот момент многие упускают из виду, так как есть срок гарантийного обслуживания, в течение которого эксплуатирующей организации не требуется использование собственных средств для ремонта и обслуживания оборудования автоматизированных систем управления. Однако, по истечении гарантийного периода подобные работы необходимо будет выполнять самостоятельно, а поиск требуемого оборудования и различных средств значительно затрудняется в связи со снятием оборудования с производства и совершенствованием техники и средств автоматизации.

Кроме того, необходимо в процессе эксплуатации проводить обучение специалистов для повышения эффективности работы и обслуживания использующихся на объекте средств и систем.

Хорошев В.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ЭЛЕКТРОННАЯ СИСТЕМА КОНТРОЛЯ БЕЗОПАСНОСТИ РАБОТНИКА НА ЖЕЛЕЗНОДОРОЖНЫХ ПУТЯХ

Железные дороги являются местом повышенной опасности. Персонал, производящий работы вблизи железнодорожных линий, подвергается различным рискам для жизни. Одним из часто встречаемых происшествий на железнодорожном транспорте является наезд подвижного состава на работника. Работники выполняют свои обязанности в тяжелых условиях труда, поэтому необходим тщательный надзор за перемещением каждого из них при выполнении своих обязанностей.

Сегодня надзор за передвижением и действиями работающего персонала производит руководитель работ. При производстве работ на перегонах, расположенных в сложных природных условиях, где задействовано большое количество персонала, задача наблюдения за безопасностью работников становится трудновыполнимой.

На полигоне российских железных дорог производится внедрение различных компьютерных систем во все технологические процессы и операции, при этом обеспечивается достижение целей исключительной безопасности движения, увеличения пропускной способности, повышения перерабатывающих способностей станций и узлов. Внедрение цифровых технологий способствует снижению стоимости аппаратуры. Развитие компьютерных систем позволяет создавать мощные производственные системы при меньших габаритах в сравнении, к примеру, с релейной техникой. Создаются новые системы мониторинга, программное обеспечение которых позволяет контролировать различные параметры устройств и операций.

Вопрос обеспечения безопасности на железной дороге имеет важнейший приоритет. Монтаж систем контроля работы оборудования производится различными фирмами и институтами. В настоящее время имеется масса подобных систем для анализа работы оборудования, но нет систем, позволяющих обеспечивать безопасные условия производства работ для персонала. К примеру, при работах на перегоне работникам на путях выдается радиостанция, а машинистам подвижных составов, работающих на том же участке железной дороги, выдается листок предупреждение о производстве работ. Данные мероприятия не являются достаточными в силу различных обстоятельств таких, например, как поломка радиостанции или утеря листка предупреждения (несовершенство технологий предупреждений).

Обозначенную проблему позволяет решить развертывание системы контроля безопасности работника на путях. Построение системы возможно несколькими вариантами, один из которых и предложен в данной работе.

Вариантом технической реализации системы контроля безопасности работника на путях является использование цифровых меток. Такими метками могут быть RFID, встраиваемые в рабочий сигнальный жилет работника или в помещаемые в браслет. Данная метка является точкой в цифровом пространстве. Устройство сигнализации в кабине машиниста реализовано в виде блока с индикацией, на экране которого отображается расстояние от подвижной единицы до работника и сигнальная пиктограмма. Если на расстоянии полного рабочего торможения находится работник на путях, то исходя из скорости подвижной единицы, система выдает предупреждение и расстояние до работника. Реализация связи между меткой работника и сигнального блока в кабине машиниста возможна по спутниковой связи, радиоканалу или при развертывании систем датчиков в районах железной дороги.

При использовании спутниковых систем вместо RFID-метки используется модуль GPS, при использовании сотовых сетей – GSM-передатчик для определения нахождения работника методом триангуляции. Из трех приведенных методов связи RFID-технология самая выходная и наименее энергозатратная, так как метка пассивная и питания не требует. Система мониторинга за персоналом с использованием меток RFID функционирует на основе установки сети из блоков на протяжении железнодорожных путей, скажем на опоры контактной сети. На борту блока имеется ретранслятор для передачи информации работнику на браслет и машинисту. На всей оборудованной территории блоки так же связываются друг с другом для передачи информации в оба направления перегона на посты ЭЦ и далее на серверы для дальнейшего использования и хранения. При выходе из строя одного или нескольких блоков на перегоне между станциями «А» и «Б» на посты ЭЦ придет сигнал об отсутствии контроля участка. По защищённому каналу информация передается от ретранслятора на антенну на локомотиве. В кабине машиниста звучит звуковой сигнал бдительности и на табло блока сигнализации высвечивается информация, на браслет с меткой от ретранслятора передается информация о приближении подвижной единицы. Для индикации приближения состава к работнику, вместе с меткой устанавливается маленький вибромоторчик.

Внедрение подобных систем мониторинга за безопасностью нахождения работника на путях способствует повышению не только безопасности движения по железным дорогам Российской федерации, но и повышению культуры безопасного производства работ на путях.

Черепанова М. Р.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

К ВОПРОСУ О СРАВНЕНИИ ХАРАКТЕРИСТИК СИСТЕМ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ, СИНТЕЗИРОВАННЫХ С ИСПОЛЬЗОВАНИЕМ КЛАССИЧЕСКИХ И ВЗВЕШЕННЫХ КОДОВ С СУММИРОВАНИЕМ

В автоматике и вычислительной технике для определения технического состояния логических схем часто используют функциональный контроль устройств. При организации систем функционального контроля наиболее важными характеристиками являются обнаруживающая способность и структурная избыточность системы. Один из часто используемых методов – использование классического кода с суммированием, или кода Бергера (далее *S*-код). У *S*-кода значения разрядов контрольного вектора представляют собой сумму единичных разрядов в информационном векторе, записанную в виде двоичного числа. Таким кодом обнаруживаются однонаправленные ошибки любой кратности и не обнаруживаются разнонаправленные ошибки четной кратности, при которых искажается одинаковое количество нулей и единиц (при таких ошибках сохраняется число единиц в информационном векторе). Обнаруживающая способность классических кодов с суммированием в системах контроля является крайне низкой, например, ими не обнаруживается 50% двукратных ошибок на рабочих выходах контролируемых схем. Повысить эффективность обнаружения искажений в информационном векторе можно за счет модификации кода по алгоритму, описанному далее. Назовем получаемый по данному алгоритму код модифицированным кодом с суммированием взвешенных разрядов (*RWSM*-кодом).

Построение контрольного вектора для *RWSM*-кода:

1. Каждому разряду присваивается вес из натурального ряда (1,2,…,*m*).
2. Вычисляется число *V* как сумма весов единичных разрядов.
3. Выбирается модуль *M.*
4. Число *V* берется по выбранному модулю $W = V(\mathrm{mod}M)$ и представляется в двоичном виде.
5. Подсчитывается коэффициент α как сумма по модулю два заранее выбранных информационных разрядов.
6. Записывается кодовый вектор следующим образом: α является старшим разрядом, а значение числа *W* – оставшимися разрядами кодового вектора.

Модуль для данного кода рационально выбирать по двум правилам:

1. Значение *M* должно быть равно степени числа два.
2. Часть контрольного вектора, отвечающая за значение *W*, должна иметь на один разряд меньше, чем контрольный вектор *S*-кода.

В коэффициенте α должны участвовать разряды информационного вектора, вес которых равен значению модуля M, в противном случае появляются однократные необнаруживаемые ошибки при искажении данных разрядов.

При сравнении показателей обнаруживающей способности S-кодов и RWSM-кодов было выявлено, что в общем случае модифицированный код в сумме обнаруживает больше искажений, чем S-код. Проведенные расчеты с кодами со значениями длин информационных векторов m=3…17 показали, что число необнаруживаемых ошибок RWSM-кода снижается в среднем в 2…4 раза по сравнению с кодом Бергера. Это связано с тем, что код Бергера не использует некоторые из комбинаций контрольных разрядов и очень неравномерно используются остальные. У модифицированного же кода каждому контрольному слову соответствует одинаковое количество информационных.

Выяснив, что RWSM-код лучше обнаруживает искажения в информационном векторе, чем код Бергера, нужно сравнить вторую важную характеристику, которую учитывают при построении систем функционального контроля – структурную избыточность.

Были проведены эксперименты на пятидесяти двух контрольных логических схемах – бенчмарках (группа MCNC Benchmarks). По результатам экспериментов было выявлено, что для схем с числом контрольных выходов $m \leq 14$ в большинстве случаев использование кода RWSM дает системы функционального контроля с уменьшенной площадью по сравнению с системами функционального контроля, построенными по S-коду. Однако при больших значениях m (m=16, m=17) S-код всегда занимает меньшую площадь, чем RWSM-код. Тем самым показано, что применение RWSM-кода в некоторых случаях оправдано.

Чертовской В.Д.
Россия, С.-Петербург, ГУМРФ им. адм. С.О. Макарова

ВОПРОСЫ ПОСТРОЕНИЯ И РЕАЛИЗАЦИИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

Одним из эффективных способов повышения конкурентоспособности в машино-, приборо- и кораблестроении является оперативный переход на выпуск новой продукции, что эквивалентно

изменению цели функционирования системы управления производством. Реакцией системы на изменение цели является изменение связей системы. Такие системы называют интеллектуальными.

Для этого специфического класса автором разработаны принципы построения, методология и обобщенная теоретико-множественная модель. Такие системы обладают трехуровневой структурой управляющей части: руководитель – диспетчер, начальники цехов Для функционального наполнения всех уровней структуры и построения математической модели системы автором предложен и апробирован однородный метод, составленный из локальных методов: статического линейного программирования и дифференциальных или разностных уравнений. уравнений.

Компьютерная реализация модели имеет два варианта: на основе реальных данных; путем генерации данных для процедуры проверки основных положений процедуры моделирования.. Поскольку идентификация реальных данных сильно затруднена, акцент делается на генерацию данных.

В реализации модели можно выделить следующие этапы: построение согласованного варианта; формирование несогласованного варианта; отражение процедуры перехода на выпуск новой продукции.

Работы на первом этапе проводятся в следующих фаз. 1. Генерируются данные уровня диспетчера, согласованные по экономическим интересам с помощью предложенного алгоритма генерации. 2. Далее на их основе составляются модели уровней руководителя и начальников цехов. 3. Для всех структурных элементов решается задача статического линейного программирования. Этот этап используется фактически для настройки компьютерной модели.

На втором этапе выполняются фазы 1 и 2. Затем при генерации вводится рассогласование интересов. Далее следует процедура согласования интересов по предложенному автором алгоритму.

На этапе 3 выполняется фаза моделирование исходного состояния при использование этапов 1 или 2. Затем на второй фазе вводятся данные процедуры перехода на выпуск новой продукции. Результаты фаз сравниваются и по предложенному критерию определяется по предложенному необходимость перехода. При положительном решении определяется и анализируется вариант перехода.

Начальная реализация проведена с применением программного продукта MatLab. Реализация показала хорошие алгоритмические возможности продукта. В то же время выявились следующие недостатки.

1. Трудности привязки алгоритмов к структуре системы из=за отсутствия сетевого варианта.
2. Затруднения ввода сгенерированных данных в алгоритмы.
2. М алая размерность модели в силу отсутствия построения высокоразмерных баз данных.

Устранение недостатков возможно при использовании режима «клиент-сервер» в варианте «тонкого клиента». Для него характерна трехуровневая структура: сервер баз данных – сервер приложений – клиенты. Сервер БД содержит базу данных, сервер приложений включает алгоритмы генерации, решения задач статического линейного программирования и согласования экономических интересов, ответы на запросы клиентов. В качестве клиентов, осуществляющих запросы к сарверу приложений, выступают руководитель, диспетчер, начальники цехов.

С позиций программной реализации названные уровни - разнородные фрагменты, которые следует интегрировать. Для этого необходимо составить требования к интегрируемым программным продуктам и осуществить их выбор. Анализ выявил возможность использования в сервере баз данных - СУБД Denver, в сервере приложений и клиентах - программный продукт Apache, языки программирования Java и html. Отдельные составляющие режима апробированы и в настоящее время ведутся работы по их интеграции.

Чухонин В.М., Осадчий Г.В., Фомин Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ИСПОЛЬЗОВАНИЕ СВОЙСТВ САМОПРОВЕРЯЕМЫХ ПАРАФАЗНЫХ АВТОМАТОВ В СОЧЕТАНИИ СО СВОЙСТВАМИ МАЖОРИТАРНОЙ ФУНКЦИИ ПРИ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Построение современных систем железнодорожной автоматики и телемеханики (ЖАТ) на компьютерной элементной базе становится общепринятой нормой. Среди многочисленных задач, решаемых разработчиками таких систем является повышение надежности программного обеспечения (ПО). Одним из направлений решения поставленной задачи является использования самопроверяемых программ базирующихся на достижениях в области аппаратной реализации.

Прежде всего, синтез передовых систем ЖАТ основан на использовании достижений теории надёжности. Одним из вариантов синтеза таких систем является использование парафазных автоматов. Обычно парафазная схема однотактного автомата строится по его однофазной реализации, построенной в базисе {И, ИЛИ, НЕ}. Каждый элемент схемы из базиса {И, ИЛИ, НЕ}, заменяется его аналогом в парафазном представлении.

В многочисленных работах рассмотрены методы синтеза парафазных автоматов при схемной реализации, однако, вопрос получения алгебраического описания парафазного автомата, необходимого для программной реализации, минуя описание по схеме, не рассмотрен.

Стоит также отметить, что использование свойств самопроверяемых парафазных автоматов в сочетании со свойствами мажоритарной функции для программной реализации является весьма перспективным

В парафазных схемах для представления двоичной переменной X в парафазном виде выделяются две фазы – линии: единичная линия с обозначением (X1) и нулевая линия (X0).

Ставится вопрос, в каком отношении находятся X1, X0 и значения переменой X в ее прямом и инверсном виде в функциях алгебры логики (ФАЛ).

Задача повышения надёжности дискретных устройств использует различные виды их резервирования. В этом случае используют восстанавливающий орган (ВО), в виде пороговой логической функции.

Проведенное исследование показывает, что все наборы таблицы истинности мажоритарной функции можно разделить на 5 групп по реакции на отказы.

Также можно получить новые мажоритарные функции для восстанавливающих органов с заданной избыточностью.

Яицкий И.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I

ПРОБЛЕМА УЧЕТА ТЕПЛОВЫДЕЛЕНИЯ ОТ РЕЛЕЙНЫХ И МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЭЛЕКТРИЧЕСКИХ ЦЕНТРАЛИЗАЦИЙ

В настоящее время актуальной является проблема тепловыделения в системах электрической централизации (ЭЦ), как релейных, так и микропроцессорных.

В релейных системах ЭЦ основным элементом является реле – прибор, рассчитанный на работу в широких диапазонах температур. Микропроцессорные же системы, в которых основные элементы имеют в своем составе большое количество полупроводниковых элементов, являются чувствительными к изменениям температуры. Проблема изменения температур до определенных пороговых значений сверху и снизу приводит к нарушениям в работе устройств ЭЦ, поэтому требуются системы охлаждения, устанавливаемые в помещениях, где функционирует сама аппаратная часть ЭЦ.

Основные недостатки микропроцессорной техники, работающей в помещении, связаны с тем, что при длительном нагреве у транзистора (это основной элемент, из которых состоит микропроцессор и любой микроконтроллер) может возникнуть пробой. При длительном тепловом влиянии же происходит разрушение транзистора. Обычно ЭЦ, основанные на микроконтроллерах, имеют пассивное охлаждение, вследствие чего им требуется дополнительное охлаждение в виде кондиционеров в помещениях поста ЭЦ (для охлаждения горячего воздуха).

Микропроцессорная централизация обычно содержит очень много микроконтроллеров, и если один из них греется, например, до 40°С, то это не будет являться слишком существенным. Однако сотня таких микроконтроллеров дадут существенную прибавку к температуре воздуха в помещении, что может отрицательно сказаться на работе системы или же привести к ее отказу. Более того, существенное повышение температуры может привести к невозможности работы обслуживающего персонала в помещении. В релейных системах ЭЦ данная проблема остро не стоит.

Система основанная на микропроцессорных решениях имеет ряд преимуществ перед релейной ЭЦ, поэтому для развития данного типа систем нужно иметь универсальный способ, для того чтобы рассчитывать тепловыделение для установки микропроцессорной централизации. Так же необходимо, что бы данный способ был универсален не только для микропроцессорных, но и для релейных систем, которые используются или проектируются в метрополитенах и на магистральном железнодорожном транспорте.

Данная проблема актуальна и у нее есть решение – разработка универсальной методики расчета тепловыделения, с помощью которой можно рассчитать тепловыделение при использовании системы основанной на реле или на микропроцессорах. Этому и посвящено предлагаемое исследование в области интеллектуальных технологий на транспорте.

Яшин М.Г., Пантелеев Р.А., Шарлай А.С., Фомин С.Н., Цуриков С.В.
Россия, Санкт-Петербург, Военный институт (Железнодорожных войск и военных сообщений) Военной академии материально-технического обеспечения

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ВОССТАНОВЛЕНИИ СТАНЦИОННЫХ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Эффективность железнодорожного транспорта зависит от пропускной и провозной способности железнодорожных участков. Для обеспечения заданных размеров перевозок и высокой пропускной

способности, а также безопасности движения поездов существуют системы интервального регулирования движения поездов (СИРДП), полноценное функционирование железных дорог без них не возможно. Вследствие этого при разрушении или выходе их из строя назревает необходимость скорейшего их восстановления. Используя современные информационные технологии можно произвести расчёт необходимых для этого сил и средств.

1. Восстановление станционных устройств автоматики и телемеханики.

Для замены разрушенных устройств автоматики, телемеханики и связи на раздельных пунктах на кафедре Восстановления устройств автоматики, телемеханики и связи на железных дорогах Военного института (Железнодорожных войск и военных сообщений) ведётся разработка «Унифицированного восстановительного комплекса (УВК-ШЧ-ТМ)» ядром которого является релейно-процессорная централизация (РПЦ), использование которого позволяет оперативно восстановить регулирование движения поездов на станции без привязки к устройствам автоматики и телемеханики до разрушения и без использования других восстановительных средств.

УВК-ШЧ-ТМ, смонтированный на базе кузовов-фургонов контейнеров постоянного и переменного объема, должен включать в себя не только постовое, но и напольное оборудование ЭЦ. В связи с этим, возникает задача расчёта оптимального количества последнего, включаемого в возимый комплект комплекса и зависящее от объёма работ, которые необходимо произвести для восстановления путей на станции на основании сведений, представленных технической разведкой.

2. Расчёт станционного напольного восстановительного комплекта.

Расчёт комплекта ведётся в зависимости от топологии и технического оснащения станции. В начале рассчитывается необходимое количество стрелочных электроприводов, затем количество датчиков информации о занятости или свободности путевых участков (предлагаются системы счёта осей подвижного состава), а затем необходимое количество светофоров.

3. Методика расчёта потребного количества сил и средств вариантов восстановления станционных устройств железнодорожной автоматики и телемеханики.

В методике на первом этапе имеет место корректировка восстанавливаемых устройств по данным результатов, зафиксированных в данных технической разведки. На втором этапе, анализируется вся исходная и расчётная информация и определяется вероятный (минимальный) станционный напольный восстановительный комплект на основе процесса исследования операций симплексным методом линейного (целочисленного) программирования, при помощи алгоритма Гомори.

На третьем этапе методики производится расчёт трудозатрат и определение продолжительности выполнения работ.

На следующем (IV этапе) предлагаемой методики, осуществляется разработка сетевого графика с использованием программы Microsoft Project.

В представленной методике расчёта потребного количества сил и средств вариантов восстановления станционных устройств железнодорожной автоматики и телемеханики получены следующие результаты:

– представлены вопросы восстановления систем автоматики и телемеханики с использованием транспортабельных модулей УВК-ШЧ-ТМ смонтированных на базе кузовов-фургонов, которые возможно доставить на разрушенную станцию различными видами транспорта и обеспечивающих наибольшие темпы восстановления, прерванного движения поездов, тем самым высокий уровень живучести железнодорожных линий и направлений;

– решён вопрос расчёта потребного минимального напольного оборудования необходимого для скорейшего открытия движения поездов на восстанавливаемой станции, где исходным значением является количество восстанавливаемых путей;

– определён состав станционных напольных восстановительных комплектов по категориям станций и выполняется выбор необходимых наборов этих комплектов для восстановления устройств автоматики и телемеханики;

– произведён расчёт трудозатрат, продолжительности восстановительных работ с разработкой сетевого графика;

Использование данной методики позволит оптимизировать и более рационально распределять ограниченный ресурс времени, материалов, человеческих сил, выделяемых на восстановление прерванного движения в различных условиях обстановки, и будет составной частью концепции восстановления систем организации движения поездов.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУЧНЫХ ИССЛЕДОВАНИЯХ

Бусыгин А.Г., Коноплев А.С.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ

На сегодняшний день основными средствами идентификации и аутентификации при управлении доступом к ресурсам децентрализованных систем являются сертификаты стандартов X.509 и OpenPGP.

Системы контроля доступа, использующие сертификаты стандарта X.509, широко используются в децентрализованных вычислительных сетях (например, в грид-системах), однако обладают следующими недостатками:

- службы удостоверяющего центра формируют единую точку отказа. Например, несанкционированный доступ к закрытому ключу любого удостоверяющего центра компрометирует всю инфраструктуру;
- закрепление идентификатора за его владельцем не гарантируется. Удостоверяющий центр обладает чрезмерно большими полномочиями. Например, удостоверяющий центр имеет возможность забрать идентификатор у одного владельца и передать другому без их согласия. Удостоверяющий центр также может злонамеренно или в результате ошибки выпустить дублирующий сертификат;
- целостность и общедоступность всех когда-либо изданных сертификатов и списков отозванных сертификатов не гарантируется, что в свою очередь может привести к невозможности проверки подписей, выполненных с помощью ключей с истекшим на момент проверки сроком действия;
- недостатки механизмов проверки отзыва сертификатов. Службы проверки отзыва сертификатов, такие как реестры списков отозванных сертификатов и службы, реализующие протокол OCSP, усложняет систему, создают дополнительные точки отказа и проблемы информационной безопасности.

Системы, основанные на сетях доверия и стандарте OpenPGP, не обладают первым из описанных выше недостатков, однако вносят дополнительную сложность, связанную с добавлением новых доверенных субъектов. Отсутствие ответственного центра усложняет установку первого отношения доверия между субъектами и часто требует личной встречи.

Предложенная модель децентрализованной системы контроля доступа обладает следующими свойствами:

- децентрализованность;
- уникальность идентификаторов субъектов;
- наличие отношений доверия;
- владелец идентификатора субъекта обладает эксклюзивными правами на данный идентификатор (идентификатор в течение своего срока действия не может быть отнят у владельца без его согласия);
- наличие и доступность механизма поиска свойств (открытых ключей и проч.) субъектов по идентификаторам субъектов;
- наличие и доступность полной истории изменений свойств субъектов и отношений доверия.

Данная модель имеет трёхуровневую структуру:

- на уровне 1 выполняется формирование упорядоченного списка транзакций;
- на уровне 2 осуществляется формирование базы, находящейся в согласованном состоянии, путём последовательного выполнения транзакций;
- на уровне 3 осуществляется поиск заслуживающей доверия информации о субъектах.

Основная сложность построения систем согласно описанной выше модели состоит в реализации уровня 1. Создание общедоступного исключительно для чтения и записи в конец журнала транзакций является нетривиальной задачей. Применение технологии Блокчейн позволяет решить данную проблему путем использования блокчейна на уровне 1 в качестве журнала транзакций и, тем самым позволяя построить децентрализованную систему контроля доступа согласно описанной модели.

Верзун Н.А., Ипатов О.С., Колбанёв А.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОПТИМИЗАЦИЯ ПРОЦЕССА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕТЯХ БУДУЩЕГО ПО КРИТЕРИЮ ЭНЕРГОЭФФЕКТИВНОСТИ

Новое направление развития телекоммуникационных сетей, приходящих на смену сетям следующего поколения next/new generation networks(NGN) – сети будущего – Future Networks(FN). Необходимость возникновения новой концепции обусловлена непрерывным изменением требований к телекоммуникациям. Сегодня появляются принципиально новые приложения (например, дистанционно взаимодействующие с умными вещами(УВ) Internet of Things), создаются «умные» сети, широко используются «облачные» вычисления и т.д. По мнению специалистов, примерно до конца текущего десятилетия (к 2020 году) должны появиться сети будущего – Future Networks. Международный союз электросвязи определяет сеть будущего следующим образом: это глобальная информационная инфраструктура, которая должна объединить в себе уже существующие ИКТ-сети с учетом компонентов, которые только планируются к внедрению, имеющая единый центр управления и способная предоставлять полный спектр телекоммуникационных услуг на базе инновационных технологий (в любом географическом месте, с гарантированным качеством, по приемлемой стоимости и в любое время).

Уже в 2011 году была принята первая рекомендация (Y.3001), описывающая основные положения FN, цели и задачи их создания. В частности, в Y.3001 уделено особое внимание факторам, которые будут влиять на создание сетей будущего. Наиболее важным из них назван экологический фактор. Экологические аспекты создания и функционирования сетей будущего затронуты также в рекомендациях Y.3021 и Y.3022. Например, в Y.3021 изложены основы энергосбережения для будущих сетей.

В соответствии с Y.3021, снизить негативное воздействие на окружающую среду (при использовании FN) можно, во-первых, путем применения FN как инструмента, который позволит снизить негативное воздействие других областей экономики на окружающую среду: «умные» энергосети smart grid, позволяющие распределять электрической мощности; всепроникающие сенсорные сети (Ubiquitous Sensor Networks), контролирующие изменения экосферы Земли; во-вторых, путем уменьшения негативного воздействия непосредственно самих FN на окружающую среду. Один из основополагающих принципов сетей будущего – экологическая чистота, и их характерной чертой является снижение потребления всеми компонентами сети. Внутри сетей будущего выделяют три уровня (устройств, оборудования, сети), каждому из которых соответствуют свои технологии энергосбережения. На уровне сети, это технологии, применимые во всей сети (алгоритмы передачи данных, сжатия, кодирования, маршрутизации и пр.).

В докладе рассматриваются сетевые технологии, в частности, организация процесса информационного взаимодействия двух УВ в беспроводной сети, с точки зрения энергии, затрачиваемой в ходе этого взаимодействия. Учитываются следующие действия: избыточное помехоустойчивое кодирование и отправка информационных блоков между УВ. Предполагается два возможных режима кодирования: 1 - обнаружение ошибок и 2 - обнаружение и исправление ошибок. Предлагаются выражения для расчета затрат энергии на взаимодействие двух УВ, с применением которых исследуется зависимость потребления энергии на помехоустойчивое кодирование информационных блоков при их передаче в беспроводной сети от коррекционной возможности кода, а также качества эфирной среды передачи.

Горбунова И.Б., Чибирёв С.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЭЛЕМЕНТОВ МУЗЫКАЛЬНОГО ТВОРЧЕСТВА

Во второй половине XX – начале XXI вв. появилось новое направление в музыкальном искусстве и моделировании закономерностей музыкального творчества, обусловленное быстрым развитием электронных музыкальных инструментов (от простейших синтезаторов до мощных музыкальных компьютеров). Возникла новая междисциплинарная сфера профессиональной деятельности, связанная с созданием и применением специализированных музыкальных программно-аппаратных средств, требующая знаний и умений как в музыкальной сфере, так и в области информатики — музыкально-компьютерные технологии. Это послужило действенной основой для построения модели музыкального творчества, позволяющей проводить анализ и синтез музыкальных текстов на основании статистических параметров фрагментов музыкальных произведений.

Отметим также усиление интереса отечественных учёных к проблеме моделирования процесса музыкального творчества в последние годы (работы С.А. Филатова-Бекмана, А.С. Фадеева, Н.Ю. Глазырина и др.), музыкальному программированию. Отдельную группу исследований составляют практические разработки, среди которых выделим работы московской компании Widisoft, в частности, программу WIDI Recognition System, предназначенную для распознавания музыки с помощью компьютера и направленную на получение читаемой нотной записи в формате MIDI из музыкальной аудио записи формата mp3 и wave. В целом, сегодня можно выделить два класса разработок в данной области: системы, сравнивающие аудио-отпечатки мелодии и системы, работающие с объектным форматом мелодии, ориентированные, как правило, на широкого пользователя. Данные системы существуют либо в виде специализированного программного обеспечения, либо могут быть интегрированы в сервисы сотовых операторов для различных мобильных устройств.

В предлагаемом подходе музыкальные фрагменты в формате MIDI (партитуры) рассматриваются как абстрактный текст. Основное внимание уделяется обработке и структуризации статистической информации, полученной при анализе текста стандартными методами. Исследования на данном этапе позволяют выделить большее количество закономерностей (по сравнению со стандартным подходом), сделать возможными моделирование и интерактивные эксперименты и в перспективе обеспечить возможность проведения семантического анализа. Такой инструмент исследования дает возможность получить конкретные результаты в следующих теоретических и практических областях:

1) построение моделей звуковых последовательностей, удовлетворяющих заданным условиям;
2) изучение особенностей восприятия звуковых сигналов как информационного потока; установление принадлежности различных звуковых фрагментов к определенным типам; установление авторства звуковых записей;
3) восстановление утраченных фрагментов звуковых записей; имитации звуковых сигналов заданного характера и т.п.

В качестве методов исследования в нашей работе используются статистический анализ, теория графов, целочисленные методы решения статистических задач. Компьютерная реализация разработанных алгоритмов производилась на основе объектно-ориентированного подхода.

Евневич Е.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОПРЕДЕЛЕНИЕ ТЕНДЕНЦИЙ РАЗВИТИЯ КОГНИТИВНЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ АНАЛИЗА ПАТЕНТНОЙ ИНФОРМАЦИИ

Идея искусственных когнитивных систем возникла примерно в середине 20 века. Спектр исследований и разработок в данной области в настоящее время очень широк: от амбициозных долгосрочных многомиллиардных европейских, американских и азиатских проектов полномасштабного моделирования человеческого мозга : «Человеческий мозг» на суперкомпьютере «Blue Gene»; карта активности мозга IBM WATSON – суперкомпьютер , когнитивная система Watson (распознавание естественного языка; IBM Cognos Analytics – система бизнес аналитики; IBM C2S2 (восприятие информации, анализ, принятие решений и т.п.). Первая фаза проекта – DARPA SyNAPSE (Systems of Neuromorphic Adaptive Plastic Scalable Electronics)(USA) – создание новой компьютерной парадигмы – «система нейроморфной адаптивной пластичной масштабируемой электроники». BRAIN Initiative или Brain Activity Map Project (BAMP) (USA) – «картирование активности мозга». Аналогичен европейскому проекту HBP. Google и NASA собираются создавать искусственный интеллект с помощью квантовых компьютеров. Brain/MINDS (Brain Mapping by Integrated Neurotechnologies for Disease Studies) (Japan), China Brain и др. и до специализированных задач по созданию обучаемых роботов-манипуляторов (i-cube, Boston dynamics, экзоскелеты и многое другое).

По результатам обзора материалов 2015 года ежегодной конференции ЕПВ (EPO Patent Information Conference) был сделан вывод об аналитическом потенциале патентной информации. Подчеркивалась важность патентных исследований для выбора перспективных направлений и составления прогнозов развития передовых технологий (прогностический потенциал патентной информации).

В процессе исследования был проведен патентный поиск по патентной базе ESPACENET в ручном режиме по ключевому слову cognitive в названии патента (title). Глубина патентного поиска в соответствии с ГОСТ Р 15 011-96 – 10 лет (2006 - 2015 г.г.).

Большинство патентов, касающихся искусственных когнитивных систем, принадлежит Китаю, Корее и США. Значительная их часть посвящена когнитивному радио и когнитивной обработке сигналов. Патенты стран Европы преимущественно касаются медицинских, физиологических, психологических и фармакологических вопросов, связанных с когнитивной функцией человека, чем обусловлено сравнительно небольшое количество европейских патентов по искусственным

когнитивным системам. Средний процент патентов по искусственным когнитивным системам по отношению ко всем патентам на когнитивную тему – примерно 50%.

Анализ патентов по когнитивным технологиям за 10 лет в мире показывает, что это направление получает серьезный импульс в своем развитии.

Текущие результаты свидетельствуют, что проблема создания полноценных когнитивных искусственных машин и систем еще далека от своего решения.

Состояние исследований по когнитивным машинам в России (судя по числу зарегистрированных патентов) не в полной мере удовлетворяет практическим нуждам.

Большие надежды в части создания когнитивных машин возлагаются на достижения в области микро- и наноэлектроники, в частности, на использование энергонезависимой мемристорной памяти.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРОБЛЕМЫ ПРОГНОЗИРОВАНИЯ КОСМИЧЕСКОЙ ПОГОДЫ И ПОЛЕТЫ НА МАРС

Планета Марс – единственная планета солнечной системы, где имеются возможности колонизации землянами, расселение землян на Марс существенно повысит устойчивость нашей цивилизации при наличии космических угроз. Первый этап движения к Марсу – это освоение Луны. Для безопасности космических полетов необходимо прогнозировать космическую погоду, которая зависит от многих факторов, и прежде всего от активности солнца. В докладе рассматриваются вопросы прогнозирования космической погоды на основе лингво-комбинаторного моделирования эволюции галактики, звездных кластеров и солнца и системного анализа с учетом фактора жизни во Вселенной.

Ипатов О.С., Колбанёв М.О., Татарникова Т.М.
Россия, г. Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Санкт-Петербургский государственный университет аэрокосмического приборостроения

НОВЫЙ ВЗГЛЯД НА МОДЕЛЬ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

В середине XX века пионерами кибернетики была определена новая методология деятельности, в основе которой лежит системный подход и кибернетическая модель управления. Эта модель разделяет реальные объекты на два блока:

- субъект управления – это источник активности. Он располагает моделью объекта и способен формулировать цели, достижение которых зависит от поведения объекта;
- объект управления – это направление активности. Он способен занимать те или иные состояния, в которых обеспечивается преобразование входящих информационных и материальных потоков в выходные потоки с определенными свойствами.

Наличие прямых и обратных информационных связей между субъектом и объектом позволяет некоторым рациональным или оптимальным путем достигнуть цели, то есть желаемых параметров выходных потоков, изменяя функционирование объекта командами управления.

Эта модель легла в основу первых автоматизированных систем управления (АСУ) процессами в экономике, а затем и процессами в других областях деятельности.

Однако, по мере развития технологий, информатизация деятельности смогла получить новое наполнение. Сначала на смену АСУ пришли информационные системы (ИС), исследование которых независимо от объекта управления стало невозможным. Один из неотъемлемых элементов ИС - это описание (модель) предметной области или, фактически, виртуальный образ объекта управления. Сегодня этот подход в полной мере реализуется в ERP системах.

По мере роста масштабов ИС, с одной стороны, и развития технологий инфокоммуникации, с другой, появилась возможность трансформировать ИС в корпоративные ИС (КИС), структурные элементы которых распределены в пространстве соответственно структуре объекта управления. В силу распределения информационных, физических и энергетических ресурсов КИС, приложение классической кибернетической модели возможно здесь лишь применительно к ее отдельным фрагментам, соответствующим некоторым структурным элементам объекта управления и содержащим информацию о функционировании именно этих элементов.

Еще одним достижением кибернетики является общая схема системы связи, которая предназначена для «точного или приближенного переноса сообщения между двумя точками пространства» (К. Шеннон). Эта модель не учитывает:

- идеальную (смысловую) сторону информационного взаимодействия, хотя она и «не имеет отношения к технической стороне вопроса» (К. Шеннон),
- процедуры формирования сообщений, результатом которых является представление смыслов в виде последовательности знаков на том или ином языке,

– особенности информационных процессов взаимодействия во времени, в пространстве и путем обработки данных,
– распределение в реальном пространстве элементов данных и пользователей,
– взаимодействие многих пользователей в реальном масштабе времени,
– физическую природу данных, преобразование которых требует реальных энергетических затрат,
– многие особенности информационных процессов в цифровой среде и др.

Однако учет этих обстоятельств становится необходимым условием при моделировании современных инфокоммуникационных систем и сетей, основанных на технологиях облачных вычислений, интернета вещей, больших данных, широкополосного мобильного доступа и наложенных сервисов. Главным ограничителем развития последних стала не сложность кодирования данных, а семантические и энергетические характеристики реализуемых ими процессов.

В докладе делается попытка построения некоторой новой модели деятельности, сочетающей методы классической и неклассической науки. Предлагаемая модель деятельности обосновывается в виде сложной интеллектуальной коммуникационной сети. Приводятся примеры, демонстрирующие область применения предложенной модели.

Колоколов Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)

ПРОБЛЕМЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ХИМИИ И МАТЕРИАЛОВЕДЕНИИ

В развитии любой науки, в том числе и химии, происходит поэтапная смена научных парадигм. Термин «парадигма научного знания» был введен Т. Куном в его работе «Структура научных революций» (1962, русский перевод – 1977). Т. Кун определяет парадигму как «признанные всеми научные достижения, которые в течение определенного времени дают научному сообществу модель постановки проблем и их решений».

Перенос информации с бумажного формата в цифровой происходит в следующей последовательности: сбор информации, хранение информации, обработка/поиск/доступ информации. Первая проблема, с которой мы сталкиваемся, это проблема идентификации веществ и соединений, а точнее обработка огромного количества материала. Так же необходимо учитывать тот факт, что вещества могут быть одного состава, но разного строения, и специалисты могут по-разному интерпретировать одно и тоже вещество как по записи, так и графически. Основываясь на этих фактах необходимо создать такую базу данных, которая бы определяла вводимые вещества, обрабатывала их, структурировала, не давая запись уже записанных веществ и соединений, и была бы настолько обширной, чтобы хранить максимально возможное количество материала.

Сразу же сталкиваемся со следующей проблемой, откуда брать информацию о соединениях, ведь помимо их строения, нам необходимо знать как физические, так и химические свойства. В своем распоряжении мы имеем различные справочные материалы, дополнительные источники. Однако этого не достаточно, потому что нужно учитывать специфические или недавно открытые вещества. В решении данной проблемы нам поможет само научное сообщество. Речь идет о научных публикациях и статьях. Но и с этим есть трудности, ведь необходимо, так же, проводить проверку этих публикаций и статей.

Теперь перейдем к проблеме визуализации строения вещества, которое, бесспорно, необходимо. Нужно учитывать как человеческий фактор, так и всевозможные способы записи данных исследований. Так же не нужно забывать об обработке строения и соотнесения информации с соответствующим веществом. К счастью, эта проблема решена. Не нужно задумываться с чего нужно начинать запись и как её вести. На данный момент существует несколько стандартов записи и расположения строения соединений. Запись необходимо начинать с центра масс и, основываясь на длинах связи и валентных углах, графически изображать строение вещества. Для такого вида деятельности и существует программное обеспечение. Существование подобных программ, безусловно, облегчает работу с уже обработанными и записанными соединениями и дает почву для последующей определения и записи веществ.

Совершенно очевидно, основными принципами научной парадигмы являются информационные технологии, которые значительно повышают эффективность обработки информации.

Кузнецова А.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПОПУЛЯРНЫЕ АЛГОРИТМЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

В связи с перманентным возрастанием количества информации в интернете становится необходимым разработка алгоритмов её обработки. Несмотря на большое разнообразие уже имеющихся механизмов обработки информации, некоторые из них получили более широкое распространение по ряду причин.

1. Деревья решений. Различные алгоритмы на основе построения деревьев. Применяются в основном для создания классификаторов. Такие алгоритмы принимают на вход коллекцию примеров, каждый из которых принадлежит какому-либо классу и описывается набором атрибутов, а в результате получается классификатор, который может определить, к какому классу относится новый пример.

2. Алгоритм k-средних. Очень популярный и простой итеративный алгоритм для разделения множества данных на заданное пользователем количество более мелких кластеров.

3. Метод опорных векторов. Довольно точный, простой и потому хорошо известный алгоритм. Состоит в классификации данных путем нахождения гиперплоскости, находящейся на максимальном удалении от каждого из классов.

4. Алгоритм Apriory. Один из распространенных алгоритмов для составления ассоциативных правил. Базируется на составлении соотношений и отношений между переменными.

5. Алгоритм AdaBoost. Алгоритм для классификации. Основной идеей является построение композиции базовых классификаторов. Основным преимуществом является то, что каждый следующий классификатор строится по объектам, которые плохо классифицируются предыдущим классификатором.

6. Метод k ближайших соседей. Один из самых простых алгоритмов классификации. Суть алгоритма сводится к тому, что объект присваивается тому классу, к которому принадлежит большинство его соседних элементов.

7. Наивный Байесовский классификатор. Принимает набор независимых объектов, каждых из которых принадлежит какому-либо классу. Целью является определить, к какому классу будет отнесен новый объект на основе вычисления апостериорной вероятности принадлежности объекта к каждому из классов. Соответственно объект относится к тому классу, для которого эта вероятность выше.

Наибольшую популярность приобретают простые алгоритмы, которые, в основном, дают точные результаты и применимы к большинству задач невысокого уровня. Однако, существуют задачи, которые требуют более сложных и точных алгоритмов, но их построение основывается на знании базовых алгоритмов.

Левшун Д.С., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

СРАВНЕНИЕ ПОДХОДОВ К ПОСТРОЕНИЮ БАЗ ДАННЫХ ДЛЯ ОРГАНИЗАЦИИ ПОИСКА МАТЕРИАЛОВ В ЕДИНОМ ХРАНИЛИЩЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ ИЗ ПОЛЕВЫХ ЭТНОГРАФИЧЕСКИХ ЭКСПЕДИЦИЙ

Полевые архивы экспедиций, как правило, насчитывают несколько сотен аудио и видеофайлов, содержащих исполнение эпичных сказаний как во время ритуала, так и под запись, интервью со сказителями, ритуальными специалистами и их родными и близкими, записи процессов изготовления предметов с ритуальным значением. Кроме того, в архивах собраны рисунки сказителей, а также несколько тысяч фотографий, которые изображают не только ритуальные моменты, но и животных, растения, а также предметы обихода, имеющие высокий семиотический статус.

Одной из фундаментальных научных проблем является разработка методов хранения, представления и поиска результатов проведенных исследований на основе привезенных из полевых экспедиций массивов разнообразных качественных данных. При этом основным фактором, влияющим на производительность, при работе с каталогами такого типа является возможность удобного поиска различных мультимедийных объектов.

Поиск информации в базе данных - это процесс отбора из общего множества информационных объектов тех, которые удовлетворяют условиям, сформулированным в запросе. Объекты могут выбираться из общего множества по значению одного идентифицирующего (ключевого) признака или по сочетанию значений нескольких из них. Они также могут выбираться по сочетанию любых других (неключевых) признаков, если это сочетание однозначно выделяет их из множества объектов.

При разработке моделей данных важно учитывать, что по содержанию метаданные могут быть формальными (описывают объект как единицу хранения) и содержательными (описывают объект как совокупность семантических единиц). Это означает, что привычный для аналоговых хранилищ принцип формального описания единиц хранения не обязательно переносить на цифровые архивы. Современные технологии позволяют организовать сложную разметку содержания объектов при помощи иерархий аналитических тэгов. В отличие от отбора объектов по формальным параметрам, содержательные метаданные предоставляют возможность аналитического поиска. Например, можно найти все объекты, отмеченные определенным тэгом, при условии, что тэги организованы в иерархии.

Для решения задачи поиска материалов в едином хранилище мультимедийных данных из полевых этнографических экспедиций в основном применяются два подхода к построению

баз данных: онтологический и реляционный. Рассмотрим достоинства и недостатки каждого из подходов более подробно.

Достоинства онтологического подхода:

– запрос к любому из информационных объектов позволяет извлечь полную информацию о взаимосвязи данного объекта со всеми другими объектами (например, запрос по фамилии этнографа позволит извлечь данные о его возрасте, образовании, месте рождения, а также обо всех экспедициях, в которых данный этнограф принимал участие, и всех мультимедийных объектах, которые были получены с его помощью).

– Недостатки онтологического подхода:

– сложная и разветвленная структура онтологии существенно снижает скорость ответа на поисковый запрос к базе данных;

– представление об описании информационных объектов у разных людей может отличаться, что может повлечь за собой появление нескольких онтологий, слабо связанных между собой.

Достоинства реляционного подхода:

– более жесткая и менее адаптивная структура, предоставляющая более высокую скорость ответа на поисковый запрос к базе данных (по сравнению с онтологическим подходом);

– Недостатки реляционного подхода:

– полная информация об информационно объекте извлекается из базы данных путем построения сложного запроса, объединяющего и, если необходимо, преобразующего несколько информационных объектов;

– хранение неструктурированных данных связано с дополнительными трудностями.

Важно отметить, что в применимости к построению баз данных для организации поиска материалов в едином хранилище мультимедийных данных из полевых этнографических экспедиций нет однозначно лучшего подхода. Как онтологические, так и реляционные базы данных обладают помимо важных достоинств и серьёзными недостатками. Именно поэтому, решение об используемом подходе должно применяться для каждого конкретного случая отдельно, например на основе наличия или отсутствия готовых решений для организации поиска материалов в едином хранилище данных.

Работа выполнена при финансовой поддержке РФФИ (проект №16-37-50073) в СПИИРАН.

Нечитайленко Р.А., Новопашин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРИНЦИПЫ ВЗАИМОДЕЙСТВИЯ ВЕБ-СЕРВИСОВ В РАМКАХ СЕРВИСНО-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ

Предметом исследования являются технологии обеспечения реализации базовых свойств веб-сервисов, описанных в примерах традиционного использования и определении оригинальных вариантов, ориентированных на производственные и исследовательские задачи. Технологический фундамент веб-сервисов образуется следующими технологиями:

– eXtensible Markup Language (XML);
– Simple Object Access Protocol (SOAP);
– Universal Description, Discovery and Integration (UDDI);
– Web Services Description Language (WSDL).

Современные тенденции ИТ технологии лежат в основе взаимодействия веб-сервисов в рамках сервисно-ориентированной архитектуры. Задача структурирования сервисно-ориентированной архитектуры решается среди трёх основных архитектурных компонента сервисно-ориентированной архитектуры:

– пользователь сервиса: приложение, программный модуль либо сервис, осуществляющий поиск и вызов необходимого сервиса из реестра сервисов по описанию сервиса, в том числе использующий сервис, предоставляемый провайдером сервиса, в соответствии с интерфейсом сервиса;

– провайдер сервиса: приложение, программный модуль либо сервис, осуществляющий реализацию сервиса в виде веб-сервиса, прием и исполнение запросов пользователей сервиса, в том числе публикацию сервиса в реестре сервисов;

– реестр сервисов: библиотека сервисов, предоставляющая пользователям сервиса средства поиска и вызова необходимого сервиса и принимающая запросы провайдеров сервисов на публикацию сервисов.

Каждый компонент в постановке задаче проектирования архитектуры может выступать в единичной роли или сложной роли: быть, например, только пользователем сервиса либо одновременно провайдером одних сервисов и пользователем других. В данном описании компонентов сервисно-ориентированной архитектуры следует различать термины "сервис" и "веб-сервис", при организации взаимодействия между ними это имеет существенное значение. Под сервисом понимается бизнес-функция, пользователь которой осуществляет поиск в реестре

необходимых бизнес-функций и формирует запросы; под веб-сервисом - программная реализация бизнес-функции (сервиса). В ходе взаимодействия друг с другом компоненты сервисно-ориентированной архитектуры выполняют следующие основные операции:

- публикация: для того, чтобы сервис был доступным (вызываемым) пользователям сервиса, необходимо сделать интерфейс сервиса известным пользователю;
- поиск: пользователь сервиса должен иметь возможность найти в реестре сервисов необходимый сервис, удовлетворяющий заданным критериям;
- связывание и вызов: после получения описания сервиса, пользователь сервиса должен иметь возможность вызвать и использовать сервис в соответствии с описанием сервиса.
- Организация выполнения основных сервисно-ориентированных операций является основой для выстраивания и согласования требуемой принципов взаимодействия конкретных веб-сервисов.

Рассматривая взаимодействие компонентов сервисно-ориентированной архитектуры необходимо отметить наличие следующих двух артефактов:

- описание сервиса: определяет формат запроса и отклика при взаимодействии пользователя сервиса и провайдера сервиса, а также требуемое качество сервиса;
- сервис: собственно сервис, который может быть вызван и использован пользователем сервиса в соответствии с опубликованным интерфейсом сервиса.

При организации работы пользователя, провайдера и пользователя с провайдером, необходимо учитывать разную направленность понятий сервис и описание сервиса, имеющих собственную специфику и отражающихся на принципах организации архитектуры.

Универсальность сервисно-ориентированной архитектуры поддерживается принятыми стандартами взаимодействия веб-сервисов. С целью выработки и популяризации стандартов, описывающих взаимодействие веб-сервисов в рамках СОА, создано международное объединение около 150 ведущих компаний, называющееся WS-I (Web Services Interoperability Organization). Важным результатом работы данного объединения стало создание и утверждение в 2003 году так называемого WS-I Basic Profile 1.0 - пакета базовых спецификаций веб-сервисов, взаимоувязанных с целью обеспечения широких возможностей взаимодействия веб-сервисов. В настоящее время в данный профиль входят следующие спецификации технологий:Кроме того, в профиле описаны сценарии, демонстрирующие основные методы организации взаимодействия между веб-сервисами.

Острейковский В.А., Демченко М.Л.
Россия, г. Сургут, Сургутский государственный университет

ТЕОРИЯ ФРАКТАЛОВ ДЛЯ ОЦЕНКИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

Рассмотрен класс математических моделей фракталов при оценке техногенного риска в теории безопасности атомных станций. Применение фрактального метода к оценке показателей техногенного риска в комплексе с известными детерминированными методами позволяет более конкретно оценивать безопасность такого сложного динамического объекта каким является атомная станция.

Острейковский В.А., Муравьев И.И., Павлов А.С.
Россия, г. Сургут. Сургутский государственный университет, Сургут, ОАО «Сургутнефтегаз», ПУ «СургутАСУнефть»,
г. Обнинск, Обнинский институт атомной энергетики – филиал НИЯУ МИФИ

МОДЕЛИРОВАНИЕ СЛУЧАЙНЫХ ПРОЦЕССОВ В ЗАДАЧАХ ОЦЕНКИ ФАКТОРА ВРЕМЕНИ ТЕОРИИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ СИСТЕМ

Исследование посвящено чрезвычайно актуальному в настоящее время направлению в теории безопасности объектов нефтегазовой отрасли. Техногенный риск является одним из перспективных критериев оценки техногенной безопасности сложных динамических систем. За последние 60 лет произошел ряд аварий и катастроф на объектах энергетики, транспорта, добычи и переработки нефти и газа. Эти аварии и катастрофы сопровождались выбросами радиоактивных токсичных веществ, пожарами, взрывами, гибелью сотен и тысяч людей, загрязнениями больших территорий водных поверхностей. Именно поэтому проблема безопасности высокотоксичных и пожаро- и взрывоопасных веществ в энергетике, транспорте и нефтегазовой отрасли требует создания фундаментальной базы анализа и обоснования безопасности сложных критически важных объектов (СКВО).

В докладе рассматривается применение корреляционного анализа случайных процессов функционирования СКВО в задачах оценивания длительности наблюдений в теории безопасности сложных динамических систем.

В рамках исследования обосновывается методика оценки фактора времени в моделях техногенного риска с использованием метода корреляционного анализа стационарных случайных процессов на этапе периода нормальной эксплуатации СКВО.

Проведенные эксперименты с обработкой больших массивов статистической информации о поведении обобщенных прогнозирующих функций оборудования СКВО показали в целом адекватные результаты оценки времени наблюдения за показателями техногенного риска.

Методика (алгоритм) корреляционного анализа фактора времени в задачах количественной оценки техногенного риска выглядит следующим образом:

1) Выбор модели корреляционной теории случайных процессов;
2) Сбор статистической информации;
3) Проверка гипотезы нормального распределения прогнозирующей функции объекта в сечении случайного процесса;
4) Проверка случайного процесса на стационарность;
5) Проверка случайного процесса на эргодичность;
6) Расчет длительности наблюдений;
7) Анализ полученных результатов и выдача рекомендаций о выборе времени наблюдений при исследовании значений показателей техногенного риска СКВО.

Острейковский В.А., Шевченко Е.Н.
Россия, г. Сургут, Сургутский государственный университет

ОБРАТИМЫЕ И НЕОБРАТИМЫЕ ВО ВРЕМЕНИ ПРОЦЕССЫ В ТЕОРИИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ СИСТЕМ

В настоящем докладе выполнен анализ обратимых и необратимых процессов на моделях оценки фактора времени в развитии теории техногенного риска сложных динамических систем. Большое внимание уделено историческому развитию постулатов количественной оценки фактора времени, которые получили большое распространение в теории риска, надежности и безопасности.

Христофоров М.В.
Россия, Санкт-Петербург, Университет ИТМО

СИСТЕМЫ ДЛЯ АВТОМАТИЗИРОВАННОГО СБОРА ДАННЫХ ИЗ ГЕТЕРОГЕННЫХ ИСТОЧНИКОВ В ОРГАНИЗАЦИИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Количество новых информационных систем, используемых в различных отраслях человеческой деятельности, с каждым годом растет, что ведет к увеличению данных, накапливаемых в процессе эксплуатации этих систем людьми. Многие из существующих информационных систем содержат встроенный аналитический функционал, целью которого является свести накопленные системой данные в форме графиков или отчетов. Однако зачастую этих возможностей оказывается недостаточно для конечного потребителя, поэтому организации могут использовать специализированные информационные системы, целью которых является сбор данных, их обработка и визуализация в необходимом формате.

В зависимости от условий и задач, имеющихся в конкретной организации, обычно могут применяться системы одного из следующих классов: BI-системы (Business Intelligence), системы мониторинга, сервисные шины предприятия. Каждый из классов имеет свои отличительные черты и их эффективное применение ограничено условиями, в которых они применяются.

BI-системы могут быть использованы для построения отчетов на основании многомерных данных, источниками для которых могут быть базы данных и отдельные файлы, расположенные на различных серверах организации. Сильными сторонами таких систем можно назвать средства визуализации, поддержка OLAP-кубов и технологии "drill-down"(возможность перехода с одного уровня данных модели на другой в один «клик» мышки), поддержка большинства распространенных СУБД и файловых форматов в качестве источников данных, а также интуитивно-понятный интерфейс, позволяющий пользователю без знаний языка SQL свести данные из различных источников. Недостатками таких систем являются отсутствие поддержки алгоритмической предобработки данных, а также высокая стоимость. Это значит, что если организация ориентирована на применение алгоритмов интеллектуального анализа на данных, доступ к которым предоставляют BI-системы, то эти алгоритмы придется применять вне самой системы. Кроме того, не всякие данные можно извлечь, используя язык структурированных запросов. Например, если в качестве источника данных выступает копия всех страниц сайта формате HTML, то отобрать только данные таблиц, встроенных в эти страницы в структурированном формате при помощи SQL практически невозможно.

Системы мониторинга характеризуются использованием частых периодичных однотипных запросов, направляемых различным информационным системам и серверам в рамках сетевой инфраструктуры организации. Нередко системы мониторинга поставляются, как распределенная система с топологией типа "звезда", где центром выступает сервер для сбора данных, а на концах лучей размещаются агенты - резиденты серверов. Преимуществами систем мониторинга является возможность следить из единого центра за тем, чтобы ключевые показатели различных систем не отклонялись от нормы, визуализация накопленных данных в виде набора графиков, универсальные агенты для любой платформы, а также возможность сравнения состояния систем в различные

временные периоды. Недостатками таких систем является ограничения при извлечении данных, а также в объеме собираемых данных. За универсальность агентов, размещаемых на серверах организации, приходится платить ограниченным функционалом. Кроме того, агенты работают все время, поэтому ресурсоемкий сбор данных может повлечь за собой существенное снижение производительности или отказ основных систем сервера. Так как данные собираются из различных серверов в едином центре, то при больших выборках данных даже с малого количества серверов размер дискового пространства может оказаться недостаточным.

Сервисные шины предприятия позволяют организовать централизованный и унифицированный обмен данными. Данные из одной системы могут быть переданы в другую систему, претерпев некую алгоритмическую обработку. Преимуществами таких систем является широкая поддержка различных источников данных, возможность их алгоритмической обработки в процессе передаче, а также поддержка событийно-ориентированного запуска тех или иных транзакций между серверами. Недостатком таких систем является отсутствие средств визуализации, собственного хранилища для сбора данных, а также высокая стоимость и сложность конфигурирования.

Представители рассмотренных классов систем не могут быть использованы эффективно, когда одновременно необходимы сбор данных из различных источников, поддержка индивидуализированных выборок данных с поддержкой сложных алгоритмов, как части процесса сбора и предобработки данных для интеллектуального анализа. В условиях неопределенности источника, неопределенности требований к отбираемым данным, а также неопределенности сетевой инфраструктуры конечной организации предлагается использовать распределенную систему для автоматизированного сбора данных, способную применять алгоритмы пользователя в процессе сбора и подготовки конечных данных. Демонстрационная платформа подобной распределенной системы под названием "EduSensors" была разработана и протестирована на ряде примеров.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена, Финансовый университет при Правительстве РФ, Санкт-Петербургский государственный институт психологии и социальной работы

МЕТОДОЛОГИЯ АНАЛИЗА, КЛАССИФИКАЦИИ И ТАКСОНОМИИ ЦЕЛЕЙ ОБУЧЕНИЯ ИНФОРМАТИКЕ И ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ В УСЛОВИЯХ ИНТЕРНАЦИОНАЛИЗАЦИИ ОБРАЗОВАНИЯ, ПОЛЯРИЗАЦИИ ЭКОНОМИЧЕСКИХ РЫНКОВ, РЕГИОНАЛЬНОЙ И ГЛОБАЛЬНОЙ МИГРАЦИИ ТРУДОВЫХ РЕСУРСОВ

В условиях интернационализации модели Болонского образования и связанного с этим интенсивного развития направлений подготовки и поколений ФГОС ВО, ВПО, стандартов профессионального образования, динамичного реформирования и слияния вузов, непрерывного изменения традиционных форм и электронных систем обучения в вузах, усложнения показателей и методик расчета эффективности обучения, поляризации экономических рынков, региональной и глобальной миграции трудовых ресурсов, происходит непрерывная и достаточно быстрая смена российских целей, оснований, теорий, классификаций и принципов обучения информатике и ИТ на региональные, международные и транснациональные (глобальные) цели, классификации и принципы обучения.

Для анализа целей обучения информатике и ИТ в современных условиях поляризации экономических рынков, региональной и глобальной миграции трудовых ресурсов и интернационализации образования предлагается использовать методику анализа на основе таксономии целей - теории классификации и систематизации сложноорганизованных в том числе научно-педагогических областей знаний.

В российской педагогике анализ целей обучения информатике и ИТ предполагает рассмотрение различных оснований: содержание изучаемого материала, деятельность преподавателя, внутренние процессы развития студентов, организацию учебной деятельности студентов на занятиях. Методология определения целей обучения информатике и ИТ с точки зрения традиционной российской педагогики состоит из следующих этапов: 1) определение познавательных и информационных аспектов информатики и ИТ; 2) определение мотивационных составляющих информатики и ИТ для студентов; 3) формирование психомоторных функционалов деятельности студентов в области информатики и ИТ. С точки зрения таксономии эти этапы можно представлять в виде областей - доменов целей обучения.

Методика классификации и методологии анализа целей обучения информатике и ИТ в современных условиях с точки зрения таксономии предполагает, что для каждой из этих групп областей - доменов необходимо разработать многоуровневые таксоны: 1) функции профессиональной деятельности; 2) профессиональные решения или сервисы обучения; 3) критерии, показатели эффективности и успешности профессиональных решений - сервисов; 4) технологии кластеризации возможных неоднородностей целей обучения информатике и ИТ; 5) методы определения взаимозависимостей целей обучения информатике и ИТ; 6) средства снижения избыточности требований и компенсации количества целей обучения в том числе компетенций по информатике и ИТ в современных условиях поляризации экономических рынков, региональной и глобальной миграции трудовых ресурсов и интернационализации образования.

Практическую разработку и реализацию таксонометрических целей обучения информатике и ИТ в настоящее время предлагается осуществлять в соответствии со следующими организационными моделями функционирования вузов при которых цели обучения (домены и таксоны):

1. Разрабатываются на основе использования российского и международного опыта, теории и методологии обучения отдельно взятого российского вуза (локальные таксонометрические цели обучения информатике и ИТ (ЛТЦОИиИТ).
2. Разрабатываются на основе использования российского и международного опыта, теории и методологии межвузовского (регионального) опыта обучения вуза (региональные таксонометрические цели обучения информатике и ИТ (РТЦОИиИТ).
3. Разрабатываются на основе использования российского и международного опыта, теории и методологии межвузовского профильного или корпоративного опыта обучения, например, консорциума экономических вузов (профильные таксонометрические цели обучения информатике и ИТ (ПТЦОИиИТ).

4. Разрабатываются на основе оптимизации региональных образовательных структур и укрепления связей образовательных учреждений высшего образования с экономикой и социальной сферой федеральных округов - федеральные таксонометрические цели обучения информатике и ИТ (ФТЦОИиИТ), разрабатываемые и реализуемые вузом совместно с международными образовательными и научными центрами, программами, ассоциациями.

5. Разрабатываются в исследовательских вузах на основе признаков эффективности образовательной и научно-инновационной деятельности, свидетельств международного и национального признания, качества, обоснованности и ожидаемой результативности образовательных и исследовательских программ на основе исследовательских и инновационных таксонометрических целей обучения информатике и ИТ (ИТиИЦОИиИТ), разрабатываемые и реализуемые исследовательским вузом совместно с международными образовательными и научными центрами, программами, ассоциациями.

6. Разрабатываются российским консорциумом федеральных и исследовательских вузов на основе конвергенции и агрегирования российского и международного опыта, теории и методологии обучения в федеральных и исследовательских вузах – конвергенциальные и агрегированые таксонометрические цели обучения информатике и ИТ (КиАТЦОИиИТ).

7. Разрабатываются на основе кумулятивных процессов, обеспечивающих формирование и усиление глобальных полюсов образовательного, экономического и технологического развития на основе накопления и концентрации образовательных процессов и научно-инновационной деятельности путём их конвергирования и агрегирования в перспективных направлениях - кумулятивные таксонометрические цели обучения информатике и ИТ (КТЦОИиИТ).

Практика показывает, что наибольшее распространение в настоящее время имеют организационные модели функционирования вузов, при которых цели обучения (домены и таксоны) ориентированы на локальные, региональные и федеральные модели высших учебных заведений. Учитывая повышение роли научных показателей и критерии оценивания вузов при разработке целей обучения информатике и ИТ преподавателям и администрациям вузов рекомендуется ориентироваться на опыт федеральных университетов и международный стандарт CS2013 - Computer Science Curricula 2013 (ACM/IEEE-CS).

Алексанова Л.В.
Россия, г. Новосибирск, Российский государственный педагогический университет им. А.И. Герцена

ВОЗМОЖНОСТИ И ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В ОБРАЗОВАНИИ

Для создания современных учебных материалов может быть использована технология дополненной реальности (Augmented reality, AR). Данная технология заключается в дополнении реального мира, расширяя воспринимаемую человеком действительность, за счёт дополнения видимого и ощущаемого мира цифровой информацией в реальном времени. С помощью AR можно преобразовать в трехмерное любое плоское изображение, попавшее в кадр. Технология дополненной реальности разделена на четыре группы по типу устройства вывода: компьютерные экраны, мобильные телефоны, встроенные в очки дисплеи и проекторы.

Педагогический эксперимент проводился на базе Новосибирского государственного педагогического университета, на факультете технологии и предпринимательства в 2014–2015 учебном году в несколько этапов. В эксперименте принимали участие студенты 1 и 2 курса направлений: профессионально обучение (по отраслям) профиль «Информатика и вычислительная техника» и педагогическое образование «Технология». Целью констатирующего эксперимента, проводившегося на первом этапе исследования, был сбор данных для анализа уровня графической грамотности у студентов первого курса, а также выявления наиболее сложных для восприятия тем по дисциплине «Начертательная геометрия и инженерная графика».

Для определения уровня графической грамотности студентов 1 курса нами был разработан тест, включающий ряд вопросов по школьному курсу черчения, охватывающие такие темы как: линии чертежа; геометрическое черчение; ортогональное проецирование, а также разрезы и сечения. На каждую тему приходилось по 5 тестовых вопросов закрытого типа.

В тестировании участвовали студенты 2х групп в количестве 42 человека. По результатам тестирования было выявлено, что 90% студентов имеют низкий уровень графической грамотности (из 20 вопросов тестирования, ошибки допустили в 12 и более вопросах).

Анализируя результаты тестирования можно сказать, что наше предположение относительно низкого уровня графической грамотности у студентов первого курса, было верным, а так же мы можем предположить, что студенты, учувствовавшие в тестировании, будут испытывать трудности при изучении графических дисциплин, таких как «Начертательная геометрия и инженерная графика».

Поэтому в рамках следующего этапа эксперимента был проведен опрос студентов второго курса факультета технологии и предпринимательства этих же направлений, с целью выявить

наиболее сложные для восприятия темы данной дисциплины. В опросе принимали участие 30 студентов 2го курса. Студентам предлагался перечень разделов дисциплины «Начертательная геометрия и инженерная графика», а так же предлагалась напротив каждой темы выставить степень сложности восприятия по 3х бальной шкале (1б – очень легко, 2б– легко. 3б– испытывал трудности, 4б– очень трудно). Исходя из результатов опроса, было выявлено, что наибольшее количество баллов набрали темы: «пересечение кривых поверхностей и объемов»; «пересечение кривых поверхностей с многогранниками»; «пересечение кривых поверхностей между собой».

Обучающий этап эксперимента был проведен в феврале – марте 2015 года на студентах направления «Педагогическое образование (профиль –Технология)» и «Профессионально обучение (профиль – Информатика и вычислительная техника)». Экспериментальное обучение проводилось в группе 1 (26 студентов). В качестве контрольной группы была выбрана 2 группа (22 студента).

Цель этого этапа эксперимента заключалась в определении повышения уровня графической грамотности у студентов при изучении дисциплины «Начертательная геометрия и инженерная графика» с применением технологии дополненной реальности. Основным критерием эффективности было выбран уровень усвоения материала. В качестве показателей были взяты отметки, полученные студентами при выполнении самостоятельной работы по построению чертежей. Задания для самостоятельной работы выдавались каждой группе сразу после объяснения лекционного материала, и предлагались к выполнению в рамках практической части лекционных занятий по дисциплине «Начертательная геометрия и инженерная графика».

В результате исследования в экспериментальной группе средний бал экспериментальной группы составил – 4,3, а контрольной – 3,5. Можно сказать, что уровень успеваемости в экспериментальной группе на 24% больше чем в контрольной группе.

Анализируя результаты эксперимента, можно сделать вывод о подтверждении предположения, что технология дополненной реальности облегчает восприятие графической информации и повышает уровень усвоения.

Экспериментальное исследование показало, что обучение студентов технических дисциплин достигает положительного результата за счет сочетания теоретических занятий с использованием компьютерных технологий, в частности технологии дополненной реальности. Это способствует развитию познавательной мотивации студентов и стремлению к получению новых знаний.

Бажукова Е.Н.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ИНФОРМАЦИОННАЯ КУЛЬТУРА КАК СРЕДСТВО ПРЕОДОЛЕНИЯ ФОРМАЛИЗМ ЗНАНИЙ ПЕДАГОГОВ-МУЗЫАНТОВ

Ситуация такова, что в век высокотехнологичных средств обучения очень быстро изменяются методики и формы организации преподавания, учителю приходится гибко владеть инновационными средствами и быстро адаптировать их к условиям с соответствующими требованиями. Педагог должен обладать информационной культурой (ИК) для применения знаний, умений и навыков работы в сетевом информационно-образовательном пространстве (ИОП) с использованием новых инструментов и технологий.

Информационная культура – данный термин применительно к обществу отражает эффективность использования информационных ресурсов и средств информационных технологий (ИТ); относительно личности – ИК рассматривается как интегративное свойство личности человека, предполагающее наличие знаний и навыков эффективного пользования информацией, что предопределяет умение целенаправленно получать нужную информацию, обрабатывать и использовать с помощью современных технологических средств и методов.

Позицию активного организатора образовательного пространства, в настоящее время, занимает преподаватель, который обладает ИК, что предполагает знание информационных ресурсов и умение вести образовательную деятельность в условиях функционирования высокотехнологичной образовательной творческой среды (ВОТС). Для полной реализации потенциала ВОТС педагог-музыкант должен знать различные модели сетевой образовательной коммуникации, формы и способы взаимодействия, средства и технологии, формы функционирования информационных и коммуникационных связей.

Понимая принцип работы в сетевом ИОП, основные цели и задачи, педагог-музыкант выстраивает обучение музыке в современных условиях, включает новые формы работы, расширяет смысловое содержание предмета, применяя при этом современные инструменты (сеть, планшет, музыкальный компьютер, синтезатор).

Таким образом, для преодоления формализма педагогу-музыканту необходимо овладеть ИК, которая включает следующие аспекты:

– сформированность знаний, умений и практических навыков к работе с использованием ИТ согласно профессионально-творческим интересам и мотивам;

– готовность к освоению ИТ (повышение информационной компетентности);
– готовность к использованию ИОП для повышения качества образования;
– умение выстроить сетевое образовательное пространство с учётом требований предъявляемых обучающимся;
– использование различных форм и видов представления информации;
– выявление логических структурных связей для целостного восприятия представленной информации;
– готовность к системности информационных знаний и овладению смысловым значением понятий.

Один из главных критериев повышения ИК преподавателя-музыканта стремление к профессиональному самообразованию, саморазвитию, самореализации.

Преодолеть формализм в освоении новых знаний в области ИТ помогут привычные для педагога-музыканта средства – МКТ и клавишный синтезатор, с помощью которых, используя знания и умения владения данными инструментами, педагог «входит» в ИОП, где процесс освоения новых знаний и умений проходит не формально, а в творческо-практической деятельности.

С помощью повышения ИК педагог-музыкант, расширит знания в области информационных технологий, овладеет современными средствами обучения (МКТ, клавишный синтезатор, планшетные технологии, интерактивные системы обучения и т.д.).

Произведя анализ средств, сетевых коммуникаций, возможности информационной образовательной среды, преподаватель-музыкант сможет осознанно, а не формально, применять знания в педагогической практике, сформировать собственную информационно-образовательную среду, опираясь на достижения в области музыкально-компьютерных технологий педагогами-практиками, будет продолжать разрабатывать методики использования данных средств и эффективно применять новые информационные технологии.

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ»

Учебная дисциплина «Инфокоммуникационные системы и сети» относится к блоку Б1 базовой части учебного плана по направлению подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (уровень бакалавриата).

В соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по указанному направлению подготовки, дисциплина поддерживает следующие компетенции:

– понимание социальной значимости своей будущей профессии, обладание высокой мотивацией к выполнению профессиональной деятельности (ОК-4);
– понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);
– способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно) для решения поставленной задачи (ОПК-6);
– способность к проектированию базовых и прикладных информационных технологий (ПК-11);
– способность разрабатывать средства реализации информационных технологий (методические, информационные, математические, алгоритмические, технические и программные) (ПК-12);

Трудоемкость учебной дисциплины составляет 180 часов, из которых 36 часов – лекционных и 36 часов запланировано на выполнение лабораторных работ.

Лабораторный практикум включает 6 лабораторных работ, предназначенных закрепить у студентов навыки практической работы с сетевыми программными и аппаратными средствами.

Лабораторная работа №1 призвана ознакомить студентов с интерфейсом программного продукта виртуализации Oracle VM VirtualBox, научить эмулировать аппаратное обеспечение ПК и устанавливать операционные системы Linux и Windows.

Лабораторная работа №2 знакомит с принципом работы протокола динамического выделения адресов (DHCP), студенты настраивают DHCP сервер на платформе Linux и клиент на платформе Windows.

Лабораторная работа №3 посвящена изучению принципов работы сетевого шлюза, студенты учатся настраивать связь между внутренней и внешней сетями, обеспечивать доступ локального компьютера в сеть Интернет, при этом меняют правила маршрутизации и исследуют прохождение пакетов через шлюз.

Лабораторная работа №4 знакомит с принципами построения сетевой системы хранения данных, студентам требуется создать NAS ресурс с доступом по протоколу SMB/CIFS.

Модуль NAS представляет собой отдельный компьютер. Основным предназначением этого компьютера является предоставление сервисов для хранения данных другим устройствам в сети.

Операционная система и программы NAS-модуля обеспечивают работу хранилища данных и файловой системы, доступ к файлам, а также контроль над функциями системы.

Лабораторная работа №5 знакомит с сетью хранения данных SAN и протоколом iSCSI, студентам требуется создать iSCSI ресурс на сервере и обеспечить доступ к нему клиентского ПК.

Сеть хранения данных (Storage Area Network, SAN) — представляет собой архитектурное решение для подключения внешних устройств хранения данных таким образом, чтобы операционная система распознала подключенные ресурсы как локальные.

iSCSI (Internet Small Computer System Interface) — протокол, который базируется на стеке протоколов TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами.

Лабораторная работа №6 посвящена знакомству с интерфейсом программы BWMeter, в ходе работы студенты учатся отображать загрузку сетевого канала и собирать детальную статистику по передаваемым пакетам данных.

Программа BWMeter предназначена для управления передачей информации по сети. С её помощью можно отображать в виде графиков загрузку сетевого канала, ограничивать скорость сетевых соединений и собирать детальную статистику по передаваемым пакетам данных.

Барышникова Н.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОРГАНИЗАЦИЯ ОБРАБОТКИ ЗАПРОСОВ ПОЛЬЗОВАТЕЛЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ЭЛЕКТРОННОГО ТЕСТИРОВАНИЯ НА ОСНОВЕ СЕМАНТИЧЕСКИХ СЕТЕЙ И ШАБЛОНОВ

На кафедре вычислительных систем и информатики ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О. Макарова» была разработана и успешно внедрена в эксплуатацию распределенная информационная система электронного тестирования для оценки соответствия профессиональным компетенциям работников морских специальностей. Реализация работы осуществлялась на платформе «1С: Предприятие 8» на основе адаптированной типовой конфигурации «1С: Электронное обучение. Экзаменатор».

Одной из основных особенностей реализованной системы является возможность внесения необходимых корректировок в организацию процесса тестирования, что важно для дальнейшего совершенствования учебных материалов и тестов. В связи с этим наибольшее внимание при создании программного продукта было отведено статистическому анализу данных, получаемых из стандартного набора отчетов информационной системы. При этом в процессе эксплуатация довольно часто встречается ситуация, когда либо полученной информации недостаточно, либо требуется более детальная расшифровка полученных результатов. Обычно для решения задач такого рода необходимо использовать средства программирования, что требует от пользователя достаточно высокой квалификации, четкого понимания структуры и наполнения базы данных, ее динамически изменяющейся структуры и объема. Пользователи системы, которыми являются как работники или претенденты на должность, так организаторы тестирований и руководители организаций, не являются специалистами в компьютерной области и испытывают сложности при получении выборки данных.

На основании этого в информационной системе был реализован формальный механизм обработки запросов, который предполагает интерактивный ввод запроса пользователем в виде произвольного текста на некотором проблемно-ограниченном подмножестве естественного языка (ЕЯ) с целью получения необходимой выборки. Его главной задачей является улучшение понимания истинного смысла введенного пользователем запроса для последующей автоматической генерации программного текста запроса.

Любой язык, в том числе и язык запросов платформы «1С: Предприятие 8», можно смоделировать на некоторой семантической сети с концептами, типы которых четко заданы предметной областью или идеологией языка. Это позволяет освободить пользователя от необходимости иметь дело с нагромождением деталей представления данных, а также сохранить их смысловую часть, при этом предоставляя независимость от выбранного метода реализации информационной системы. Еще одним преимуществом семантической сети данных является то, что она ориентирована на распознавание семантики, что дает возможность системе более осмысленным образом отвечать на поступающие входные запросы на ЕЯ. Такая модель служит более эффективным посредником между многочисленными вариациями запроса пользователя с одной стороны, и многочисленными внутренними представлениями данных с другой стороны. Каждому элементу семантической сети соответствует некоторый фрагмент исходного текста запроса. Все слои модели языка запросов платформы «1С: Предприятие 8» образуют довольно сложную сеть. В случае, когда у слоя имеется более одного предшественника, возможны коллизии в реализации сходных или зависимых концептов, введенных изначально в предыдущих слоях. Концептам, отражающим

одинаковые по смыслу данные, соответствуют аналогичные по синтаксическому строению фрагменты исходного текста запроса. Это позволяет использовать шаблоны для дальнейшей работы по обработке запроса на ЕЯ.

Каждый шаблон описывает синтаксическую структуру части исходного текста запроса на ЕЯ и создаваемые элементы семантической сети. При описании синтаксической структуры указываются не только связи слов в предложении, но и условия, накладываемые на каждое из слов. Эти условия могут проверять как лексические или семантические характеристики слова, так и смысловые пометки этого слова, заданные при поиске в других шаблонах. Если какая-то часть текста удовлетворяет всем условиям, указанным в шаблоне, то происходит ее формализация.

В заключении стоит отметить, что созданная база знаний языка запросов платформы «1С: Предприятие 8», для которой, по имеющимся сведениям о синтаксисе языка, построена семантическая сеть и целая система шаблонов, позволяет существенно сократить и упростить процесс получения требуемой информации.

Барышникова Н.Ю., Егоров А.Н., Крупенина Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ В РАМКАХ ИЗУЧЕНИЯ ЯЗЫКА ЗАПРОСОВ СРЕДЫ «1С: ПРЕДПРИЯТИЕ 8»

Современный мир характеризуется высокими темпами развития и внедрения информационных технологий, которые затрагивают различные сферы как научной, так и практической деятельности. В частности, они становятся неотъемлемой частью образовательного процесса ВУЗа, предоставляя качественно новые возможности его совершенствования и сопровождения на основе разработки и внедрения автоматизированных информационных систем, включающих в себя средства учета и контроля качества подготовки студентов. Необходимость в использовании подобных систем возникает при удаленном обучении и тестировании знаний студентов. В этой связи актуальной становится задача разработки системы дистанционного образования и тестирования, с реализацией в ней необходимого в рамках образовательного процесса функционала.

В качестве программного продукта для реализации информационной системы была выбрана платформа «1С: Предприятие 8», основой для прикладного решения послужила разработанная фирмой «1С» типовая конфигурация «1С: Электронное обучение. Экзаменатор». В ней предусмотрено использование открытых вопросов, требующих от студента заполнения полей ввода ответами. В частности, это касается лабораторных работ в рамках изучения языка запросов среды «1С: Предприятие 8». Студент с помощью текстового редактора набирает в поле ввода текст запроса, а информационная система должна корректно интерпретировать запрос, выполнить его и выдать конечный результат для последующей проверки преподавателем.

Для этого в информационной системе определена общая база совокупности возможных запросов. В каждом запросе имеются две обязательные секции – это секция описания запроса и секция источника данных запроса, а также одна необязательная – секция задания условий выборки запроса, которая может отсутствовать в исходном тексте запроса. В секции описания запроса определяется список полей, которые будут содержаться в результатах выполнения запроса и являться шапкой для таблицы результата, в секции источника данных запроса – список источников данных-таблиц, которые являются поставщиками данных, в секции задания условий выборки запроса – условия, влияющие на выборку данных в запросе. Все это в совокупности образует единую базу знаний языка запросов среды «1С: Предприятие 8», для которой, по имеющимся сведениям о синтаксисе языка, построена целая система шаблонов.

Шаблоны позволяют перевести запрос студента, представленный в свободной форме, в программный запрос к информационной системе и выполнить его. Каждый шаблон программного кода описывает синтаксическую структуру части исходного текста запроса. Если какая-то часть текста запроса студента удовлетворяет всем условиям, указанным в шаблоне, то происходит ее формализация. Если в запросе обнаруживается неформализуемая часть текста, то фиксируется ошибка, и текст запроса отправляется обратно студенту на доработку, при этом происходит подсчет числа попыток, которые могут быть учтены при выставлении оценки.

Любой запрос на языке запросов среды «1С: Предприятие 8» имеет вид, который можно свести к шаблону, например, самый простой запрос к одной таблице имеет в рамках шаблона примет следующий вид:

ВЫБРАТЬ <список_полей> ИЗ <таблица_источник>

При этом список полей, список таблиц источников данных и список условий при их наличии задаются множеством слов из входного запроса студента. После выполнения запроса информационной системой выводится результат в виде таблицы с именами столбцов, приведенных в секции источника данных и определяющими составные части шаблона.

Основное отличие между шаблонами информационной системы заключается в наличии или отсутствии:

- фильтра;
- упорядочивания:
- группирования.

Определение вида шаблона из представленных в информационной системе происходит по следующему алгоритму. По умолчанию сначала информационная система в исходном состоянии начинает работу с использования самого простейшего шаблона «ВЫБРАТЬ … ИЗ …». По мере уточнения и разбора входного запроса шаблон может изменяться на другой. При этом в новый шаблон передаются все данные из предыдущего.

Белов Г.Г.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургская государственная консерватория имени Н.А. Римского-Корсакова

ОБРАЩЕНИЕ К КОМПЬЮТЕРНЫМ ТЕХНОЛОГИЯМ В МУЗЫКЕ - НЕИЗБЕЖНЫЙ ФАКТОР ВРЕМЕНИ: РАЗМЫШЛЕНИЯ КОМПОЗИТОРА

Если в начале XXI века среди известных композиторов Санкт-Петербурга накал споров о необходимости овладения музыкально-компьютерными технологиями (МКТ) образованием был довольно повышенным и категоричным в неприятии самой постановки этой проблемы (вспомним высказывания Б. Тищенко, Ю. Фалика, Г. Фиртича в их интервью музыковедам), то сегодня учебные планы на композиторских отделениях музыкальных вузов страны обязательно включают дисциплины освоения студентами МКТ-программ. Ведь помимо того, что владение современными компьютерными технологиями заметно интенсифицируют процесс создания творцом музыкального произведения в его нотном (или только звуковом) окончательном варианте, сам композитор получает возможность от первого до последнего звука слухом и зримо контролировать всю фактуру своего опуса: убедиться в слаженности формы, отсутствия фальшивых нот, приготовить распечатку нотных партий в совершенном издательском формате и много других преимуществ. Ныне студенты бывают огорчены, если на зачётах и экзаменах им отказывают в использовании музыкального компьютера (мол, знания и умения должны быть прежде всего в голове, а не в цифровом накопителе или интернетовском справочнике).

Должно, однако, заметить, что и само обучение музыке стало более наглядным и широким (аудио и видеодиски записи классики в лучшем исполнении, нотные материалы, извлекаемые из библиотек интернета: пользуйся, не ленись!). Скорее есть опасность – утонуть в океане возможностей, если отсутствует хорошо продуманная стратегия обучения музыканта ремеслу, а затем – мастерству. Естественно, что способности, талант ученика остаются главной гарантией его продуктивного воспитания, а его художническое отношение к миру, живая, чувственная реакция на традиции и новаторство в искусстве – будут определять его успехи в становлении собственного оригинального стиля. Можно с уверенностью сказать, что компьютерные технологии здесь – не помеха, а скорее дружественный помощник.

Бергер Н.А., Яцентковская Н.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургская государственная консерватория имени Н.А. Римского-Корсакова

ФУНДАМЕНТАЛИЗАЦИЯ МУЗЫКАЛЬНОГО ОБРАЗОВАНИЯ: ИНФОРМАЦИОННЫЙ ПОДХОД.

Применение информационных технологий в музыке, становление и развитие МКТ породили новые направления в художественной сфере. Музыкальный компьютер (МК) как инструмент творчества начинает занимать всё больше места в музыкальной деятельности академического направления. Его пользователями становятся композиторы, исполнители, освоившие электронные музыкальные инструменты и формирующие новые принципы отбора репертуара, и педагоги. В среде последних МК оказывается востребованным прежде всего в дисциплинах, связанных непосредственно со слушанием музыки: музыкальной литературе, истории музыки, музыкальной формы. Гораздо меньше МК задействован в преподавании музыкально-теоретических дисциплин. Исключением, подтверждающим правило, является разработка системы тембровых диктантов для дисциплины сольфеджио, где МК фигурирует как звуковоспроизводящая аппаратура, а подход к изучению дисциплин опирается на принципы контекстуального анализа. Иначе говоря, в музыкально-образовательной сфере высокие информационные технологии функционируют, далеко не исчерпывая давно открывшихся возможностей.

Преподавание теоретических дисциплин с использованием музыкально-компьютерных технологий (МКТ) требует от педагога не только владения МК и знания основ акустики и психоакустики, но и умения осмыслить и логически объяснить те компоненты музыкальной ткани, те слагаемые собственно музыкального языка, которые и делают музыку высоким искусством, раскрывают её эстетическую сторону, наполняют смыслами и чувством. МК станет полноправным

инструментом в музыкальном образовании при условии формализации средств выразительности, как исполнительских, так и композиторских. Под исполнительскими средствами понимаются факторы управления фразировкой, такие как динамика, агогика, артикуляция, индивидуальная тембральная палитра инструмента или голоса.

Композиторские же средства условно можно разделить на три основных составляющих: пространственную (ладомелодические и ладогармонические структуры), временную (ритмические соотношения) и колористическую (обобщённые тембры инструментов). Ещё раз подчеркнём, что деление это сугубо условное, так как, например, музыкальная форма – категория пространственно-временная, а к колористическим относятся не только тембровые, но и ладово-функциональные интонационные аспекты.

Особенно важными для музыканта становятся способность объединять отдельные элементы в целостные структуры и умение оперировать ими в практической исполнительской, творческой и педагогической деятельности. Именно способность определять внутреннюю логику традиционных и нетрадиционных структур различного порядка, объединять их в системные комплексы, позволяет музыканту-творцу либо осознанно и произвольно находиться в рамках конкретной системы, либо выходить за её пределы.

Фактически речь идёт об информационном подходе к освоению музыкального языка прежде всего на основе принципов интертекстуального анализа. При информационном подходе заучивание набора элементов (звук-нота, звукоряд, лад, тональность, интервал, аккорд) уступает место выявлению их внутренних структурных закономерностей. И, через это, объединение отдельных элементов в целостные системные комплексы: все виды звукорядов и ладовых структур, типовые (частотные) мелодические и гармонические обороты, ритмические модели, пространственно-временные аспекты музыкальной формы и др. Особенно важно в сфере образования выявление, осмысление и объяснение роли компонентов музыкального языка в формировании музыки, музыкальной ткани и как процесса, и как эстетического объекта.

В век цифровых технологий необходима фундаментализация музыкального образования. Она не может исходить лишь из традиционных феноменологических принципов. Требуется значительное углубление логического, конструктивного начала в его обязательном взаимодействии с эстетической составляющей музыкального языка, что обусловливает возникновение и применение нового информационного подхода ко всем областям теории музыки.

Верхолат А.М.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ИНФОРМАЦИОННО-ПРОГРАММНЫЙ КОМПЛЕКС ВЫЯВЛЕНИЯ ПЛАГИАТА В КУРСОВЫХ ПРОЕКТАХ ПО ТЕХНОЛОГИЯМ БАЗ ДАННЫХ

В процессе подготовки бакалавров по направлению 09.03.01 «Информатика и вычислительная техника» по общеобразовательной дисциплине «Базы данных» студенты выполняют курсовой проект (КП) в соответствии с индивидуальным заданием. Курсовое проектирование состоит в разработке информационно-программного комплекса (ИПК), обеспечивающего ввод, накопление, хранение и обработку данных по заданной предметной области.

Для объективной оценки уровня знаний студента, выполнившего курсовое проектирование, преподавателю необходимо иметь представление о том, насколько самостоятельно студент выполнил КП и не заимствовал его из сети Интернет или у студентов старших курсов. При этом заимствование программного кода возможно на уровне всех компонентов проекта. С учетом этого, а также ввиду сложности КП для объективной оценки уровня знаний студента требуется весьма значительное время по каждому проекту. Для того чтобы сократить время проверки и упростить выявление плагиата в КП на кафедре систем управления и компьютерных технологий университета разрабатывается ИПК выявления плагиата в КП.

В докладе рассматриваются вопросы структурного и алгоритмического построения ИПК выявления плагиата в КП применительно к проектам, выполненным в программной среде Visual Fox Pro версий 6.0-9.0.

ИПК предназначен для выявления плагиата для следующих компонентов КП:

- структуры базы данных проекта и данных, загружаемых для проверки работоспособности комплекса;
- программного кода (ПрК) экранных диалоговых форм;
- ПрК модулей обработки запросов к базе данных;
- ПрК модулей функциональной обработки и информационно-справочного поиска;
- ПрК модулей документального вывода данных.
- Процесс выявления плагиата в КП состоит в сравнении эталонного КП с соответствующими компонентами проверяемого КП и включает следующие этапы проверки:
- ввод директория проверяемого проекта с файлами соответствующих компонентов;

– проверка на совпадение имен программных компонентов, а также на плагиат структуры и данных базы данных;

– последовательная проверка на плагиат ПрК модулей КП и отобранных компонентов эталонных КП.

Первоначальный анализ имен файлов программных компонентов, структуры и данных базы данных позволяет в существенной мере сократить перебор компонентов эталонных КП. Это определяется тем, что совпадение имен файлов программных компонентов, имен таблиц, атрибутов и их описаний в проверяемом КП и эталонном КП уже вызывает подозрение на наличие плагиата в программном коде проверяемого КП.

Результаты каждого шага проверки выводятся преподавателю в удобном для последующего анализа виде. Таким образом, ИПК обеспечивает проверку и подготовку результатов анализа на плагиат компонентов КП, а решение того, насколько выявленные результаты на плагиат могут иметь место в КП, принимает преподаватель.

В процессе анализа результатов проверки компонентов КП преподаватель имеет возможность непосредственно войти в среду Visual Fox Pro, запустить менеджер проекта, открыть сравниваемые проекты и более детально оценить степень совпадения ПрК компонентов проверяемого и эталонного КП.

Разработка ИПК выявления плагиата в КП находится в настоящее время в стадии алгоритмизации и отработки отдельных программных модулей комплекса в среде СУБД Visual Fox Pro.

Основные результаты, полученные в процессе проектирования ИПК, могут быть в дальнейшем использованы для разработки аналогичных комплексов выявления плагиата в КП, программно реализованных в других средах разработки.

Воронов А.М., Криводонова Ю.Е.
Россия, Санкт-Петрубург, Российский государственный педагогический университет им. А.И. Герцена,
Екатеринбург, Уральский государственный педагогический университет

МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ ЛЮДЕЙ С НАРУШЕНИЕМ ЗРЕНИЯ

В современном мире спектр возможностей в области получения и обработки информации значительно расширился, в том числе и за счёт применения информационных технологий. В сферу музыкального творчества также прочно вошёл мультимедийный компьютер, музыкально-компьютерные технологии (МКТ), имеющие особую значимость для музыкантов с нарушением зрения. Для них они являются средством осуществления контактов с «внешним миром» и особенно необходимы для реализации собственных возможностей и адаптации в современной социальной среде.

С одной стороны, музыкальный компьютер позволяет более эффективно изучить разнообразный по содержанию и способам представления учебный материал, с другой, – достигать положительных результатов обучения за более короткий срок. С помощью МКТ реализуется индивидуальный подход в обучении, поскольку студенты могут самостоятельно настраивать некоторые параметры обучения: устанавливать скорость освоения, объём и степень сложности материала. Применение в обучении студентов с нарушением зрения МКТ стимулирует и повышает мотивацию. Неудачи не смущают, наоборот, появляется желание их преодолеть.

Процесс преподавания МКТ незрячим людям обусловлен, с одной стороны, тем, что компьютер облегчает незрячему человеку доступ к информации разного рода, с другой, – сложностью комплекса психических реакций лиц с глубокими нарушениями зрения. Проблема обучения незрячих современным МКТ заключается также и в том, что данный контингент разнороден по типу имеющихся зрительных патологий, по виду нарушения зрения (тотальная слепота или порциальная), по времени наступления дефекта: слепота врождённая или приобретённая и так далее. При этом каждая группа незрячих, объединяемая на основе тяжести зрительной патологии, характеризуется наличием тех или иных психических особенностей, которые преподавателю информационных и коммуникационных технологий необходимо иметь в виду. Знание этих особенностей поможет грамотно и точно выдавать материал, необходимый для изучения той или иной группе реабилитантов. В докладе рассматриваются классификации людей с нарушением зрения: исходя из особенностей протекания заболевания глаз (катаракта, атрофия зрительного нерва, глоукома и т.д). В своем исследовании мы придерживаемся классификации лиц со зрительной патологией, разработанной учёными и педагогами-исследователями кафедры практической коррекционной психологии Уральского государственного педагогического университета, которые выделяют шесть групп слепых и слабовидящих людей по степени выраженности зрительного дефекта:

На основании приведенной выше классификации групп лиц по степени выраженности у них зрительного дефекта, работа преподавателя, направленная на обучение незрячих современным МКТ, должна быть построена с учетом индивидуального подхода как к каждому человеку в отдельности, так и ко всем выделенным группам в целом.

Гавронская Ю.Ю, Оксенчук В.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ВИРТУАЛЬНЫЕ ХИМИЧЕСКИЕ ЛАБОРАТОРИИ В ВУЗОВСКОМ ОБРАЗОВАНИИ

Виртуальные химические лаборатории, виртуальный эксперимент, виртуальные лабораторные работы по химии — это новая перспективная область в химическом образовании, привлекающая к себе внимание обучающихся и педагогов. Актуальность внедрения виртуальных лабораторий в учебную практику обусловлена, во-первых, информационными вызовами времени, а во-вторых, нормативными требованиями к организации обучения, то есть образовательными стандартами.

Виртуальную лабораторию в обучении химии мы понимаем как компьютерную имитацию учебной химической лаборатории, реализующую ее основную функцию — проведение химического эксперимента в образовательных целях. Химический эксперимент является специфическим средством обучения химии, выполняя функции источника и важнейшего метода познания, он знакомит учеников не только с объектами и явлениями, но и методами химической науки. Технически функционирование виртуальной лаборатории обеспечивается программно-аппаратными средствами компьютерной техники, дидактически – содержательно и методически обоснованной системой предположений о течении изучаемого химического процесса или проявлений свойств химического объекта, на основе которой разрабатывается один из возможных вариантов реакции виртуальной лаборатории на действия пользователя. Виртуальная лаборатория выступает в роли элемента высокотехнологичной информационной образовательной среды, являясь средством создания и выполнения виртуального эксперимента.

Развитие информационного образовательного пространства, образовательных сред университетов, предметных сред обучения отдельным дисциплинам создает условия встраивания в учебный процесс виртуальных лабораторных работ. Особую привлекательность им придает возможность безопасного самостоятельного проведения учащимися химического эксперимента в удобное для них время. Под виртуальной лабораторной работой по химии мы понимаем виртуальный химический эксперимент в виде совокупности опытов, объединенных общей целью изучения химического объекта или процесса, при этом студент оперирует образами веществ и компонентов оборудования, воспроизводящими внешний вид и функции реальных предметов.

Виртуальные лабораторные работы в обучении химии в вузе могут успешно использоваться как на аудиторных занятиях, так во внеаудиторной работе. На лекциях как виртуальный демонстрационный эксперимент, подтверждающий рассматриваемые положения или теории, или как средство создания проблемной ситуации; на практических занятиях для изучения качественных или количественных закономерностей протекания химических процессов. При этом возникают вполне обоснованные сомнения в целесообразности подмены реального химического эксперимента, который является уникальным специфическим средством обучения химии и вызывает неподдельный интерес учащихся, виртуальным. В этой связи мы придерживаемся мнения о том, что в аудитории виртуальный эксперимент оправдан лишь при отсутствии необходимых реактивов и оборудования или невозможности соблюсти правила безопасного обращения с ними. Еще одним доводом может служить экономия материальных средств и аудиторного времени, поскольку виртуальный эксперимент не требует покупки химикатов, измерительных приборов, установки вытяжной вентиляции и тому подобного, в большинстве случаев все процессы протекают моментально или могут быть существенно ускорены по сравнению с реальными.

Наиболее эффективным способом использования виртуальных химических лабораторий является поддержка внеаудиторной самостоятельной работы студента по химии. Во внеаудиторной самостоятельной деятельности виртуальные химические лаборатории могут работать как интерактивные задачи или симуляции натурных экспериментов с целью подготовки к лабораторной работе в аудитории. Виртуальные лаборатории как интерактивные задачи визуализируют ситуацию и предполагают активное участие студента в формировании условия, затем следует расчетная часть и актуальная проверка правильности решения. При использовании виртуальных лабораторных работ в процессе обучения химии для самостоятельная подготовка учащихся к выполнению натурной лабораторной работы часть нагрузки в формировании практических умений по химии может быть перенесена на виртуальные лабораторные работы.

В всех случаях решающую роль играет свойство интерактивности этого средства обучения, выражающееся в способности интенсивного продуктивного двустороннего взаимодействия: возможности ученика/студента вмешаться в происходящее на экране компьютера, например, выбрать тот или иной реактив, задать условия — концентрацию, объем, температуру, а также реакции компьютерной программы на действия пользователя, а именно в визуализации протекания процесса — изменении цвета, выпадении осадка, изменении показателей на приборах (pH, электропроводность, давление и т.д.).

Говорова А.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ МУЗЫКЕ НОТНОЙ ГРАМОТЕ УЧАЩИХСЯ-ИНВАЛИДОВ ПО ЗРЕНИЮ

В настоящее время инклюзивное образование неразрывно связано с применением информационно-компьютерных технологий. Для людей с ограниченными возможностями здоровья (ОВЗ) использование мультимедийного компьютера не только является средством осуществления контактов с «внешним миром», но и способствует реализации их творческого потенциала и более успешной адаптации в современной социальной среде. Музыкальное образование является одной из сфер, в которой благодаря применению музыкально-компьютерных технологий (МКТ) стало возможным обучение различных категорий людей с ОВЗ – по слуху, зрению, нарушению опорно-двигательной системы и даже интеллекта. Однако особое значение приобретают МКТ в обучении незрячих музыкантов.

Одной из важнейших особенностей обучения музыке людей с глубокими нарушениями зрения является применение рельефно-точечной нотации (разработана в середине XIX века французским педагогом Л. Брайлем и до настоящего времени постоянно совершенствуется в связи с введением новых обозначений). Брайлевская нотопись, с одной стороны, позволяет довольно точно отображать обычные (плоскопечатные) ноты, располагая развитым арсеналом обозначений, а с другой стороны, значительно отличается от последней рядом характерных особенностей, влияющих на восприятие нотного текста (отсутствием графического отображения звуковысотности и вертикали, линейностью записи и т. д.).

В специализированных музыкальных учебных заведениях, обладающих необходимыми методическими и техническими ресурсами, освоение рельефно-точечной нотации происходит в рамках особой дисциплины – «нотной грамоты по системе Брайля». На уроках учащиеся не только овладевают технологией нотной записи рельефно-точечным шрифтом, но и развивают и совершенствуют навыки разбора и игры с листа нотного текста. Комплексное изучение точечной нотации дает учащимся с глубокими нарушениями зрения возможность получения полноценного музыкального образования.

При совместном обучении людей с глубокими нарушениями зрения и людей без ОВЗ, проблема работы незрячих учащихся с нотным текстом встает достаточно остро, особенно на начальных этапах обучения. Поскольку большинство преподавателей обычных ДМШ и ДШИ не владеют Брайлевской нотацией, работа с музыкальными произведениями происходит главным образом по слуху, без использования нот. Такой подход к освоению музыкальных произведений влечет за собой снижение общего профессионального уровня, приводит к потере творческой самостоятельности в освоении новых произведений и делает практически невозможным самообразование музыканта с глубокими нарушениями зрения.

В настоящее время представляется возможным решить проблему освоения нотной грамоты по системе Брайля музыкантами с ОВЗ по зрению, а также вопрос профессионального общения (возможности беспрепятственно работать с нотным текстом) незрячего учащегося и зрячего педагога и наоборот с помощью МКТ. Данную проблему необходимо решать, как на методическом, так и на аппаратно-программном уровне, поскольку выбор доступных для незрячих пользователей МКТ-программ весьма ограничен. Подавляющее большинство современных компьютерных программ, в том числе музыкальных, имеют графическую основу и принципиально не могут работать с программами речевого доступа и Брайлевскими дисплеями, благодаря которым люди с глубокими нарушениями зрения получают возможность самостоятельно пользоваться мультимедийным компьютером.

Программы, имеющие неграфическую основу (Sonar, Band-in-a-Box и т. д.), требуют дополнительные приложения для корректной работы с речевыми синтезаторами. Педагогу, обучающему незрячего студента, необходимо четко представлять, с какими МКТ-программами учащийся может работать; кроме того, ему следует также знать, как эти программы функционируют с применением компьютерной клавиатуры, а не мыши, какими «горячими клавишами» они оснащены. С другой стороны, представляется необходимым создание такого программного обеспечения, которое было бы доступно как незрячему пользователю, так и пользователю без ОВЗ, учитывая возможности их применения с помощью речевых синтезаторов и Брайлевских строк. Немаловажным направлением является адаптация уже существующих программ для незрячих музыкантов.

Наиболее востребованным направлением представляется разработка нотных редакторов, способных конвертировать плоскопечатный нотный текст в Брайлевский и наоборот. Задачей подобной разработки является создание технической основы для адекватного профессионального общения преподавателя без нарушений зрения и незрячего учащегося на всех ступенях музыкального образования. Наличие такого программного комплекса открывает перед незрячим преподавателем музыки новые возможности работы с учащимися или студентами без ОВЗ по зрению, тем самым значительно расширяя границы его профессиональной деятельности.

Голоскоков К.П., Чиркова М.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ПОРТФОЛИО СТУДЕНТА ВУЗА

В настоящее время во многих высших образовательных учреждениях портфолио студентов создаются вручную. Это трудоемкий и неоперативный процесс, занимающий большое количество времени. Ежегодно в университетах проводятся научно- практические конференции, творческие и профессиональные конкурсы, олимпиады и т.д. Всю информацию о результатах проведенных мероприятиях необходимо собирать, систематизировать и хранить на протяжении длительного времени. И благодаря развитию информационных технологий появляются широкие возможности по автоматизации описанного выше процесса. В качестве средства автоматизации данной деятельности может выступать информационная система, позволяющая вести учёт и проводить анализ участий и достижений студента, иными словами, «Электронное портфолио студента». Нельзя не упомянуть об актуальности разработки и ведения информационной системы учета и анализа результативности участий студента в олимпиадах, конференциях, семинарах, конкурсах, соревнованиях и др. вследствие введения Федеральных государственных образовательных стандартов высшего образования (ФГОС ВО). Кроме того, положениями ФГОС ВО предусмотрено обеспечение доступа обучающихся к электронной информационно- образовательной среде организации, одной из функциональных возможностей которой является формирование электронного портфолио студента. Цель реализации «Электронного портфолио студента» (далее – ЭПС) - автоматизация процесса учёта и анализа участия и достижений студентов в мероприятиях различной направленности: научно-исследовательские, учебные, спортивно-оздоровительные, культурно-досуговые и др. Перейдем к описанию процесса учёта и анализа достижений обучающихся для определения задач, которые система должна будет решать. Каждый семестр декану предоставляется информация о существующих заслугах студентов с целью поощрения студентов за достижения в учебной, научно-исследовательской, общественной, культурно-творческой и спортивной деятельности. Затем вся эта информация анализируется сотрудниками деканата и предоставляется в виде отчётов, содержащих актуальную и достоверную информацию о студентах и их достижениях. Для того, чтобы обеспечить своевременное взаимодействие деканата и студентов, необходимо систематизировать полученную информацию. Мы считаем, что создание и ведение электронного портфолио студента обеспечит выполнение бизнес-процесса учёта и анализа результативности деятельности студентов, а также позволит снизить трудозатраты и повысить производительность должностных лиц, занятых в организации учебно-воспитательной работы со студентами. К задачам, которые должна выполнять система электронного портфолио студента относятся: 1. Учёт данных о принимаемых участиях в олимпиадах, конференциях, семинарах, конкурсах, соревнованиях. 2. Анализ информации и данных для составления отчётов. 3. Поиск студентов, которые могут принимать участие в мероприятиях. 4. Рассылка приглашений участия в мероприятиях. Ожидаемым результатом внедрения электронного портфолио является повышение продуктивности обработки данных о достижениях студентов образовательной организации, уменьшение времени поиска необходимой информации и студентов, удовлетворяющим критериям отбора, оперативное информирование потенциальных участников мероприятий. Для решения поставленных задач следует рассмотреть следующие варианты автоматизации: 1. Приобретение существующей системы; 2. Приобретение и адаптация готового приложения; 3. Разработка нового приложения. К сожалению, в настоящее время на рынке информационных систем не существует готовых приложений, которые учитывали бы требования поставленной задачи и специфику работы университета, а адаптация подходящих продуктов почти равносильна созданию нового приложения, следовательно, варианты приобретения приложения не целесообразны и силу отсутствия данной категории программных средств на Российском рынке информационных технологий. Вариант разработки ЭПС «под ВУЗ» позволит учитывать специфику образовательной организации, соответствовать особенностям внутренних бизнес- процессов подразделения. Кроме того, это обеспечит модернизацию и расширение функциональной части системы в дальнейшем, и возможность взаимодействия с другими установленными программами и приложениями. В результате проектирования электронного портфолио студента должны быть разработаны база данных для хранения информации, удобный пользовательский интерфейс, обеспечена поддержка сторонних приложений. Также следует реализовать поддержку информационного взаимодействия студентов с преподавателями. В конечном итоге будет создана информационная система, позволяющая осуществлять учет и анализ результативности участия студента в учебной, научно- исследовательской, общественной, культурно-творческой и спортивной деятельности.

Гончарова М.С.
Россия, Санкт-Петербург Российский государственный педагогический университет им. А.И. Герцена

МОБИЛЬНОЕ ОБУЧЕНИЕ В СИСТЕМЕ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГА-МУЗЫКАНТА

В отечественном музыкальном образовании сложилась уникальная система по подготовке профессиональных музыкантов и приобщения подрастающего поколения к музыкальному искусству и творчеству, основанная на многовековых классических традициях и народной музыке. Помимо этого, на новый уровень вышла инновационная музыкальная педагогика, связанная с применением музыкально-компьютерных технологий (МКТ) – современного и эффективного средства повышения качества обучения музыкальному искусству на всех уровнях образовательного процесса (ДШИ, ДМШ, средние, высшие заведения).

Современные информационные технологии в музыке и МКТ создают условия для подготовки музыкального деятеля и педагога-музыканта, владеющего кроме традиционных дисциплин музыкальным компьютером (МК) как новым специальным инструментом музыканта, позволяют гибко и разносторонне использовать богатый педагогический инструментарий традиционного обучения музыке и безграничные возможности МК. Интеграция МКТ в образовательный процесс требует подготовки педагогов нового типа, профессионально владеющих специализированными музыкальными программно-аппаратными средствами, инновационными методиками и технологиями.

На фоне постоянной содержательной модернизации профессионального образования, обновления профессиональных компетенций и повышения уровня подготовки система повышения квалификации педагога-музыканта требует большей пластичности, наличие модульных программ. Необходимо формирование нового мышления и расширения функций педагога-музыканта, который должен быть компетентным, готовым к непрерывному профессиональному росту и самосовершенствованию.

В свете описанных проблем мы рассматриваем мобильное обучение (использование мобильных устройств вне зависимости от места и времени) в системе повышения квалификации педагогов-музыкантов. Отвечая концепции непрерывного профессионального образования, мобильное обучение являются частью расширенной сферы современного образования, созданной благодаря технологиям, поддерживающим гибкое, доступное обучение, позволяющее формировать индивидуальную образовательную траекторию для профессионально-личностного роста с использованием современных информационно-коммуникационных технологий.

Несмотря на обширные исследования в области мобильного обучения, на сегодняшний день мобильные технологии практически не внедрены в учебный процесс. Как правило, тормозящим фактором в их использовании является ограниченность технологических ресурсов, равно как и быстрые изменения в образовательной, экономической и политической системе. Ещё в 2010-м году в Аналитической записке ЮНЕСКО «Мобильное обучение» упоминалось, что педагогам необходимо использовать мобильные технологии для индивидуального обучения и в подготовке обучающих материалов, а также для обмена данными и результатами исследования. Сегодня наблюдается недостаточная ИКТ-компетентность и слабая подготовка педагогов-музыкантов к методам мобильного обучения, которое охватывает мобильную педагогику, технические знания и навыки, позволяющие использовать уже существующие мобильные приложения; создание интерактивной поддержки учебного процесса, развитие ИКТ-компетенции самих обучающихся и т.д. Отсутствие методической базы и сопровождения учебной деятельности, также является причиной пассивного использования мобильных технологий в самообразовании и педагогической деятельности.

По мнению исследователя Макарчук Т.А. отличительной чертой мобильного обучения является ориентация на сознательную самостоятельную работу, и успешность обучения зависит от построения информационно-образовательной среды, основным элементом которой является «электронный образовательный ресурс в электронно-цифровой форме», включающей в себя структуру, предметное содержание и метаданные о них.

Таким образом, для реализации мобильного обучения в системе повышения квалификации педагогов-музыкантов необходимо создать благоприятную информационно-образовательную среду с определённой морально-психологической обстановкой с методическим, организационным и психологическим комплексом поддержки, обеспечивающим введение инноваций в образовательный процесс. Их первостепенным результатом является не только теоретическое и практическое овладение специалистом новшеств, но и включение этих технологий в процесс деятельности, умение успешно ориентироваться и создавать обучающую среду с их применением. Чёткое представление о содержании и критериях мобильного обучения, владение методикой применения позволяют объективно оценивать и прогнозировать их внедрение в систему повышения квалификации, предоставляя максимальные возможности для выбора и реализации индивидуальных образовательных траекторий педагога-музыканта.

Графов А.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

На данный момент существует несколько групп взглядов, зачастую противоречивых, на роль и место дистанционных образовательных технологий (ДОТ) в современной образовательной системе Российской Федерации. Например, по мнению авторов «Концепции создания и развития единой системы дистанционного образования в России», сеть дистанционного обучения (ДО) не является антагонистичной по отношению к существующим очным и заочным системам обучения, так как она естественным образом интегрируется в эти системы, совершенствуя и развивая их, способствует развитию непрерывного образования населения. С другой стороны, часто эксперты в профессиональной педагогической среде сравнивают ДОТ с одной из форм заочного обучения, выделяя при этом такие их недостатки, как: отсутствие личного общения с преподавателем и другими студентами, а также недостаток практических занятий; отсутствие постоянного контроля над студентами, что в случае недостаточно сильной мотивации и учебной дисциплины обучающегося приводит к снижению успеваемости; не все профессии подходят для дистанционного обучения ДО.

Как видно из вышесказанного, недостатки у ДОТ есть. Тем не менее, назвать их проблемами в полном смысле этого слова нельзя, т.к., во-первых, при достаточной мотивации обучающегося и наличии технических возможностей (например, специального программного обеспечения для проведения видео-конференций и др.) и выбора специальности, подходящей для данного вида обучения, удаётся компенсировать названные недостатки, а во-вторых, эти проблемы «перекрываются» преимуществами, присущими ДОТ, главными из которых являются: доступность обучения независимо от удалённости обучающегося от учебного заведения; безотрывность обучающегося от производства; меньшая стоимость такого вида обучения от классического заочного и, в особенности, – очного; значительное снижение затрат обучающегося на дорогу в учебное заведение; возможность выбора обучающимся оптимального темпа обучения, времени года, возраста и т.д.

Процесс преодоления проблем, исторически возникавших при появлении ДОТ, предопределил тенденции развития этих способов обучения, сложившихся под влиянием научного прогресса, развивающихся технических средств и информационно-коммуникационных технологий.

Одной из тенденций развития ДОТ является сетевое ДО, которое базируется на использовании локальных сетей и сети Интернет с применением мультимедийных технологий и гиперссылок на разнообразные информационные источники по изучаемой теме и сайты образовательного заведения. Сетевое ДО и массовые онлайн-курсы (например, НОЧУ ДПО «Интуит») делают обучение большого количества студентов почти индивидуальным.

Отметим, что наиболее развитой формой организации ДОТ является Виртуальный университет (ВУ) - самостоятельное учебное заведение, независимое от какого-либо учебного учреждения. ВУ предоставляет образовательные услуги исключительно методами ДО, через компьютерные сети - через глобальную сеть Internet или корпоративную сеть Ethernet. Отличительной особенностью виртуальных университетов является наличие собственной лицензии, учебных программ и курсов, а также отсутствие зданий, учебных лабораторий, студенческих общежитий, кабинетов. ВУ состоит из двух уровней - центрального университета и региональных центров. Центральный университет осуществляет административную, учебно-методическую, информационную, техническую и правовую координацию региональных образовательных учреждений. Региональный центр реализует полный цикл образовательных услуг с использованием кейс-, ТВ- или сетевых технологий в регионе.

Мировые тенденции, сложившиеся в сфере образования, характеризуются все большей открытостью и общедоступностью, демократизацией и интенсификацией процесса образования и предполагают экспорт и импорт образовательных услуг, адекватных современному информационному обществу. Конкуренция на рынке образования ведется не только между российскими вузами, но и с зарубежными организациями, что также способствует быстрому росту качества ДОТ.

Давлетова К.Б.
Россия, Санкт-ПетербургЦентр творческого развития и гуманитарного образования детей «На Васильевском»

ОСНОВНЫЕ КОМПОНЕНТЫ СОВРЕМЕННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГА-МУЗЫКАНТА

Новые технологии оказывают все более активное влияние на изменение образовательной среды. Робототехника, виртуальная реальность, искусственный интеллект, нано-инженерия и другие современные явления меняют структуру и содержание образования.

Федеральный закон РФ «Об образовании в РФ», государственные программы развития образования определяют основные направления развития системы образования и условия взаимодействия педагогов, родителей, обучающихся и социальных партнеров. Образование приобретает новое качество. Реализация такого образования связана с «открытостью информационного пространства», с развитием информационно-образовательной среды.

Информационно-образовательная среда (ИОС) характеризуется как «совокупность информационных и образовательных решений, способствующих созданию условий успешной реализации целей интеллектуального, духовно-нравственного, творческого, физического и профессионального развития человека, удовлетворения его образовательных потребностей и интересов.

Современные стандарты предполагают переход к новому уровню образования на основе применения информационных технологий. Информационная подготовка, включающая в себя владение средствами современных компьютерных технологий, в том числе и музыкальных цифровых технологий, становится одной из базовых компетенций педагогов-музыкантов и проявляется при решении ими профессиональных задач. Владение информационными технологиями, музыкально-компьютерными программами, использование возможностей цифровых музыкальных инструментов в образовательном процессе позволит педагогу-музыканту получить возможность доступа к большому объему учебной и научной информации; детализации и обобщения информации различного характера, квалифицированное и многократное использование новой информации в процессе самообразования и практической деятельности расширяет возможности обучения, в том числе и в музыкальном творчестве. Данные требования полностью могут быть реализованы только в условиях учебного процесса в ИОС, основанной на использовании средств ИКТ.

Для педагога-музыканта в ИОС появляются условия обновления форм, средств, технологий и методов реализации образовательных программ. Появляется возможность внедрения и использования музыкально-компьютерных технологий и цифровых музыкальных инструментов в образовательный процесс, и приобщения, таким образом, современных детей и подростков к высокой музыкальной культуре, сочетая традиционное музыкальное образование с инновационным. Это означает, что основной целью и задачей создания ИОС является обеспечение перехода образования в новое качество.

Основные компоненты ИОС педагога-музыканта:

– цифровые музыкальные инструменты, рабочие станции, музыкально-компьютерные программы, информационные технологии как основной элемент информационно-образовательной среды.

– учебно-методический комплекс, включающий в себя и электронные образовательные ресурсы.

– методика, разработанная на освоение и применение музыкальных технологий и возможностей цифрового инструментария в образовательном процессе, адаптированная социальным запросам педагогов, родителей, детей.

– средства измерения, оценки и контроля знаний, умений и навыков (отслеживание результатов образовательной деятельности).

Дмитриева Л.М., Батенькина О.В.
Россия, г. Омск, Омский государственный технический университет

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЦЕНТР ДИАГНОСТИКИ УРОВНЯ РАЗВИТИЯ И КОРРЕКЦИОННОГО ОБУЧЕНИЯ ДЕТЕЙ ДОШКОЛЬНОГО ВОЗРАСТА С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ»

Эффективность использования информационных технологий в процессе обучения в настоящее время не вызывает сомнений. Данные специальных исследований и официальной статистики свидетельствуют о явно прогрессирующем ухудшении состоянии здоровья подрастающего поколения, идёт устойчивая тенденция к увеличению числа детей с отклонениями в развитии, с инвалидностью. Острота проблемы определяется тем, что в настоящее время только в России насчитывается почти 2 млн. таких детей (8% всей детской популяции), из них около 700 тыс. составляют дети-инвалиды. Происходит ежегодное увеличение численности данной категории граждан.

До настоящего времени государственная социальная политика ориентирована в основном на изоляцию детей с ограниченными возможностями и содержание их в закрытых стационарных учреждениях интернатного типа. Основой данного традиционного подхода выступает то, что в условиях специального (коррекционного) образовательного учреждения таким детям можно создать оптимальную среду для развития, обучения и воспитания.

Как показывают исследования психологов и специалистов по коррекционной педагогике применение компьютерных технологий, а именно детских обучающих игр, является перспективным в образовании детей с ограниченными возможностями здоровья. Существует большое количество

образовательных программных комплексов и Интернет-порталов для детей дошкольного возраста, но эти информационные системы обучения в складывающейся тенденции не учитывают соответствующих особенностей восприятия детей с ограниченными возможностями здоровья.

Существующие развивающие и обучающие игры для дошкольников сложно отнести к диагностическим программам, поскольку только опытный специалист по работе с детьми, будь то педагог или психолог, может сделать вывод о состоянии развития ребенка по наблюдениям за его действиями.

Компьютерные же диагностические программы должны решить следующие задачи:

- установить уровень умственных способностей детей;
- оценить уровень развития психических и психофизиологических свойств личности;
- определить уровень психофизиологической и социальной готовности к поступлению детей в детский сад или школу;
- диагностировать динамику утомления ребенка в процессе занятий;
- диагностировать отклонения развития детей от нормального уровня.

Информационных систем полноценной психологической диагностики уровня развития детей дошкольного возраста с ОВЗ в настоящее время практически не существует, так как для проведения качественной оценки необходимо наличие психолога.

Современные методики психологической диагностики позволяют количественно оценить уровень развития познавательной сферы: мышления, восприятия, памяти, внимания и воображения. Некоторые из этих методик реализуются только в присутствии психолога, так как специалист может оценить эмоциональное состояние ребенка и уровень развития его эмоционально-личностной сферы в процессе диагностики. При этом используемые методики диагностики не позволяют сформировать понимание закономерностей процесса развития ребенка, так как не психолог не имеет возможности отслеживать эмоциональное состояние ребенка в процессе обучения. Данные недостатки тестирования возможно исправить с помощью видеозаписи всего процесса диагностики или обучения ребенка и последующей оценки методами распознавания эмоций.

Использование информационного портала открывает принципиально новые возможности диагностики и обучения детей дошкольного возраста с ОВЗ:

- адаптивное тестирование (вид теста, в котором каждое последующее задание выбирается в зависимости от ответов на предыдущие задания, последовательность заданий и их количество в таком виде теста определяется динамически);
- анализ данных с типологизацией объектов тестирования не по заранее заданным на основе теоретических представлений классам, а на основе эмпирических, выявляемых в ходе исследования закономерностей;
- использование временных параметров тестирования и обучения;
- использование мультимедийных стимулов, средств виртуальной реальности, игровой мотивации;
- создание базы данных и систем управления базами данных (СУБД);
- создание экспертных обучающих систем;
- самоконтроль поведенческого реагирования.

В целом, создание и внедрение информационного Центра позволит получить ощутимые положительные эффекты:

- повысить четкость, тщательность и чистоту психологического исследования за счет увеличения точности регистрации результатов и исключения ошибок обработки исходных данных, неизбежных при ручных методах расчета выходных показателей;
- обеспечит возможность проводить в сжатые сроки массовые психодиагностические исследования путем одновременного тестирования многих испытуемых;
- позволит ребенку быть более откровенным и естественным во время тестирования;
- позволит использовать время не только как управляемый параметр теста (возможность регулировать и устанавливать требуемый темп психодиагностического тестирования), но и в качестве диагностического параметра (например, показатели временной динамики ответов испытуемого на вопросы психодиагностического теста могут выступать как индикаторы утомления, эмоционального шока и т.п.);
- возможность распространять опыт работы психологов, педагогов-дефектологов за счет компьютерной интерпретации результатов тестирования;
- возможность систематически накапливать и хранить не только данные об ребенке, но и сами результаты тестирования, тем самым разрешение проблемы потери психодиагностической информации, характерной для тестирования с помощью «бланковых» тестов, осуществляется благодаря заполнению базы данных диагностируемых детей, являющейся неотъемлемым атрибутом информационного портала;
- позволит сформировать индивидуальную траекторию обучения ребенка по итогам результатов диагностики и обеспечит доступность дошкольного образования для данной категории детей вне зависимости от места проживания семьи.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-47-550894.

Дубенецкий В.А., Кузнецов А.Г., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОБЛЕМЫ АДАПТАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ БАКАЛАВРОВ И МАГИСТРОВ ПО НАПРАВЛЕНИЮ "ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ" К СОВРЕМЕННЫМ СТАНДАРТАМ CDIO

Подготовка бакалавров и магистров по направлению "Информационные системы и технологии“ сопряжена со следующими специфическими проблемами:

1. Постоянное расширение областей применения информационных систем и технологий. Вместо изучения различных областей применения требуется осваивать информационную технологию анализа, применимую к любой области применения.

2. Непрерывное и быстрое развитие и совершенствование информационных технологий. Расширяющийся спектр используемых моделей, методов и инструментов проектирования информационных систем (ИС). Необходимо найти более высокий уровень абстрагирования при описании, позволяющий единым образом представить как существующие, так и вновь создаваемые методологии проектирования ИС.

3. Существенное разнообразие классов информационных ресурсов. Необходимо найти подходящий уровень абстрагирования при изучении классов информационных ресурсов, что позволит исключить дублирование и уменьшить сложность изучения за счет использования механизмов наследования.

4. Наличие существенного разрыва между доменом проблемы и доменом решения. Необходимо использовать технологии проектирования ИС, ориентированные на использование доменных языков высокого уровня, позволяющие существенно сократить разрыв между доменом проблемы и доменом решения.

Особенностью деятельности по рассматриваемому направлению является наличие разрыва между исходными данными для разработки информационной системы и ее реализацией. Этот разрыв может быть преодолен путем получения промежуточных результатов, названных метамоделью проблемы, и метамоделью проектных решений.

Одна из главных задач обучения бакалавров и магистров по направлению «Информационные системы и технологи» является получение знаний и умений, которые позволят применять декомпозицию и абстрагирование проблемы предметной области через анализ для получения метамодели анализа, и далее от нее к реализации системы.

На каждом из этапов создания системы могут применяться разнообразные методологии и инструменты.

Выделены следующие цели адаптации:

1. Приведение содержания и результативности образовательных программ по направлению в соответствие с уровнем развития современных технологий и ожиданиями работодателей.

2. Согласование содержания образовательных программ с моделями информационных технологий, представленными в современных стандартах и рекомендациях.

3. Расширение спектра используемых моделей, методов и инструментов проектирования ИС.

Для достижения этих целей предлагается решить следующие задачи:

1. Провести анализ имеющихся стандартов и рекомендаций с целью выделения компонентов для включения в учебные планы и рабочие программы дисциплин.

2. Расширить спектр изучаемых моделей и методов решения задач управления деятельностью, разработать универсальный подход к их описанию и изучению.

3. Расширить спектр изучаемых инструментов проектирования и реализации.

4. Обеспечить детальное изучение основных классов информационных ресурсов.

5. Разработать комплексы лабораторных работ, практических заданий и курсовое проектирование, использующие проектный подход.

Предлагаются следующие направления адаптации образовательных программ по рассматриваемому направлению:

1. Усиление связей теории и практики. Используются рекомендации CDIO.

2. Согласование состава, аспектов рассмотрения и моделей изучаемых классов информационных ресурсов. Используются модели управления информационными ресурсами ITIL, IEEE 1471 .

3. Согласование состава, аспектов рассмотрения и моделей изучаемых классов изделий. Используются модели PLM.

4. Согласование состава изучаемых моделей и методов анализа информационных систем и технологий. Используем модели IEEE 1471

Ежгуров В.Н., Доброрадова В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ВНЕДРЕНИЕ И РАЗРАБОТКА СМС ИНФОРМИРОВАНИЯ В ВЫСШЕМ УЧЕБНОМ ЗАВЕДЕНИИ

На данный момент большинство учащихся используют для общения мобильный телефон. Помимо дополнительной функции – доступа в интернет, сохраняется такая функция как отправка и получение смс сообщений. В рамках развития образовательной деятельности университета предлагается реализация функционала смс оповещения обучающихся о событиях и мероприятиях университета, результатах и событиях приёмной кампании в рамках существующих информационных систем университета.

Для реализации данного функционала потребуется решить несколько задач: первая, заключение договора с мобильным оператором для отправки сообщений; вторая, программная реализация.

Задача заключения решается на юридическом уровне, и дальнейшие вопросы решаются с привлечением юристов.

При программной реализации функционала смс оповещения следует решить:

- кто и когда имеет доступ – настраиваемая политика разграничения прав доступа к функционалу;
- о каких событиях и мероприятиях следует информировать получателя – хранение истории рассылки информации и возможность рассылать информацию схожего содержания или обновления информации тем же адресатам;
- формирование групп рассылки – функционал должен позволять формировать группы рассылок, редактировать и хранить их.

Следует определить требования к интерфейсу программного продукта, так как следует исходить из того, что уровень компьютерной грамотности будет разным, а именно:

- удобный и понятный интерфейс;
- высокая скорость работы.

Дополнительным требованием к реализуемому функционалу является интеграция с базой данных абитуриентов, обучающихся и работников университета.

Так же, стоит внедрить в функционал «Кнопка отказа» от получения рассылки смс уведомлений, так работник университета или обучающийся сможет избежать нежелательной рассылки.

Также должна быть реализована функция автоматического перевода контактов из одной категории в другую. При этом человек может состоять в нескольких категориях одновременно. Изначально выделим следующие категории:

- абитуриент – категория, получаемая пользователем при подаче документов в приемную комиссию;
- учащийся – категория, получаемая пользователем после зачисления;
- выпускник – категория, получаемая пользователем после завершения обучения (в данной категории реализуется минимальная рассылка информации, зачастую несущая информацию о памятных датах и встречах выпускников);
- работник – категория, получаемая пользователем после заключения трудового договора.

Такой функционал позволит повысить оперативность и эффективность работы университета. А также повысить качество обслуживания.

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРАВОВОЙ АСПЕКТ ВНЕДРЕНИЯ В УНИВЕРСИТЕТЕ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ

В связи с внедрением в образование информационных технологий, таких как тестирование, дистанционное обучение или проведение записи защит диссертационных советов, требуется разработка новой нормативно-правовой базы. При внедрении автоматизированной системы аудио и видео записи потребуется разработать целый ряд документов, которые будут регулировать деятельность системы в юридическом аспекте.

Для разработки документов следует обратиться к опыту, который был получен специалистами: во-первых, следует обратиться к законодательным актам Министерства образования и науки Российской Федерации. Разрабатываемые документы не должны нарушать приказов и разъяснений министерства.

Также следует внимательно изучить нормативно-правовые документы и регламенты, созданные в рамках процесса проведения и оценки ЕГЭ. И самое главное, требуется изучить документы, относящиеся к проведению аудио и видео записи судопроизводства.

В список изучаемых документов должны попасть как регламенты, которые позволят точно сформировать регламенты работы автоматизированной системы, так и юридические документы, которые позволят подготовить документы к судопроизводству или досудебному разбирательству. Последний аспект очень важен, так как в документах должно быть четко прописано, в каком виде следует хранить записи и как их присовокуплять к материалам дела для судебного разбирательства.

Главная задача разработки документов – это сделать возможным защиту прав как учебного заведения, так и учащегося. И при выявлении факта недобросовестного формирования оценки учащемуся учебное заведение принимает меры, и/или документы направляются на разбирательство. Также и в случае, если учащийся и/или его законные представители начинают оказывать давление на учебное заведение, то формируется пакет документов и направляется на разбирательство.

Следует проработать юридический аспект, благодаря которому сформированные в результате работы системы документы смогут однозначно являться доказательной базой при обращении в суд.

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ВНЕДРЕНИЯ СИСТЕМЫ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ

Основы всех современных достижений всегда закладываются в образовании. Для того чтобы проверить качество полученных знаний, применяются два вида проверки: тестирование и опрос. При тестировании и опросе появляются две фундаментальных проблемы: списывание и человеческий фактор – отношение преподавателя к учащимуся. Полное устранение этих проблем почти невозможно, но в качестве меры снижения частоты появления этих проблем предлагается организовать аудио и видео запись таких контрольных событий, как зачеты/экзамены и предзащиты/защиты дипломных работ/проектов.

Данный проект с технической точки зрения предлагается разделить на несколько задач, а именно: подготовка учебных помещений для размещения аудио и видео записывающего оборудования, выделение оборудования для хранения записанных событий, формирование закрытой системы для доступа к записанным событиям и прикрепления к ним каких-либо характерных данных, на основе которых можно организовывать поиск.

Первым шагом станет оборудование аудитории на постоянной основе средствами аудио и видео записи. При оборудовании аудитории потребуется определить, сколько и какого уровня камеры потребуются для того, чтобы фиксировать происходящие в аудитории: обучающихся, подготавливающихся к ответу – цель зафиксировать факт списывания, если он будет иметь место, фиксация преподавателя и обучающегося, чтобы точно идентифицировать преподавателя и обучающегося. Далее потребуется определить средства аудиозаписи и их количество, чтобы фиксировать звуки в аудитории, вопросы преподавателя и ответы обучающегося. Также потребуется определить количество преподавателей, которые могут проводить экзамен в одной аудитории.

Вторым шагом будет выделение серверного пространства, на котором будут храниться все записи. Такое хранилище должно быть защищено от доступа извне. Сервера должны находиться в стенах университета, а доступ осуществляться только с компьютеров кафедр, деканатов, проректоров и ректоров. При этом доступ к данным возможен только на просмотр. Записи должны быть защищены от изменения и удаления.

Третьим шагом будет являться внедрение автоматизированной системы управления проведения контрольных событий. Такая система должна позволять формировать сетку расписания экзаменов на основе данных из деканата. Система будет автоматически включать запись всех событий в подготовленной для проведения контрольного события аудитории согласно расписанию. Запись будет прекращаться после команды от преподавателя, либо с терминала в аудитории – компьютер преподавателя, либо терминала на кафедре. Каждому контрольному событию в сетке расписаний будут соответствовать такие данные, как наименование события, дата и время начала, аудитория, список обучающихся и результаты. На основе внесенных данных будут формироваться отчеты по контрольным событиям.

Четвертым шагом будет интеграция созданной автоматизированной системы с другими, внедренными в учебное заведение, что позволит обмениваться данными и снизить ошибки в результате человеческого фактора.

Разработка мобильного приложения для данной автоматизированной системы и возможность расширения возможностей системы за счет организации трансляций будет рассматриваться только после внедрения автоматизированной системы и согласно нормативно-правовой документации учебного заведения и Министерства образования и науки Российской Федерации.

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ОБОСНОВАНИЕ ВНЕДРЕНИЯ В УНИВЕРСИТЕТЕ СИСТЕМЫ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ

Все больше современных технологий находят свое применение в образовании. Большинство из них направлено на обучение учащихся и студентов, а именно на облегчение учебного процесса – упрощение доступа учащегося или студента к источникам информации. Такое направление применения информационных технологий представлено в дистанционном обучении.

Но на современном этапе требуется сделать шаг в другую сторону: в сторону контроля полученных учащимся знаний. На данный момент существует ряд важных для российского человека мероприятий, направленных на контроль полученных знаний (к примеру, ЕГЭ, ГИА, защита дипломной работы или проекта и др.). В большинстве таких контрольных точек обучения сейчас внедряется или внедрено тестирование знаний учащегося, где пользователем автоматизированной системы, фиксирующей результаты учащегося, выступает сам студент – прямое тестирование за персональным компьютером, либо обработка части итоговых результатов, выданных учащимся – автоматизированная проверка ЕГЭ.

Но даже в таких "стерильных" условиях учащиеся не застрахованы от двух вещей: целенаправленного списывания и некорректной оценки знаний. Решением первой проблемы явилось формирование строгих правил проведения экзамена и фиксация проведения экзамена на видео, вторая же проблема решается в юридическом ключе – каждый несогласный со своей оценкой может подать обжалование, и тогда его дело будет рассматриваться отдельно.

Но что делать, со стандартными экзаменами или защитой дипломов в высшем учебном заведении, где предвзятое отношение преподавателя может сказаться на итоговой оценке? Введение тестовой системы оценки знаний студента позволяет исключить человеческий фактор при проведении тестирования, так как оценку проставляет система, а не человек. Но не для всех случаев это достижимо, к примеру, защита диплома или экзамен, на котором преподаватель может просто из-за человеческого фактора не поставить заслуженную оценку студенту или студент может списать.

Для таких случаев на базе аудиторий университета, относящихся к преподавательским кафедрам, предлагается внедрить систему аудио и видео записи таких контрольных точек обучения студентов как: проведение зачетов/экзаменов, проведение предзащит и защит дипломных работ/проектов. Такая мера позволит достоверно получать по запросу информацию о студентах. Реализация данного проекта предполагает, прежде всего, два фундаментальных аспекта: первое, разработка регламентов и нормативно-правовых документов по проведению аудио и видео записи, а также приведение документов к виду, пригодному для использования в юридических органах Российской федерации, второе, подготовка технической инфраструктуры для реализации надежной и защищенной системы аудио и видео записи. Так как записанные данные должны быть одновременно легкодоступны и защищены от незаконного доступа.

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет

ПРЕДЛОЖЕНИЯ ПО ВНЕДРЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СОВМЕСТНОЙ РАБОТЫ С ДОКУМЕНТАМИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

В современных реалиях самым распространенным способом общения между людьми является телефон. При этом у большинства людей, занятых в сфере как образования, так и в сфере бизнеса имеется смартфон на базе одной из операционных систем Android или iOS. В настоящее время связь и доступ к информации являются критически важными, ровно как и возможность выполнять работу совместно. Предлагается реализовать мобильное приложение для автоматизации проведения совместного рассмотрения документов и проведения голосования по вопросам совещательных мероприятий. Также будет реализована серверная часть, размещаемая на серверах образовательного учереждения.

Безопасность данных Системы предлагается обеспечивать следующими средствами:

1. Средства защиты от несанкционированного доступа:

1.1.Аутентификация пользователей планшетных и мобильных устройств.

1.2.Авторизация пользователей планшетных и мобильных устройств.

2. Средства защиты данных при передаче по открытым сетям:

2.1.Защищенный канал передачи данных между планшетным и мобильным устройством и сервером.

3. Средства защиты данных при хранении в дисковом пространстве устройства.

Для документов системы – целостность, подлинность и отказоустойчивость обеспечивается средствами формирования и проверки усовершенствованной электронной подписи.

Для обеспечения конфиденциальности информации, хранящейся на планшетном и мобильном устройстве, предлагается использовать СКЗИ «КриптоПро CSP 4.0». Данные будут шифроваться по асимметричной схеме в соответствии с ГОСТ 28147-89, на основе сессионного ключа шифрования, создаваемого на основании закрытого ключа и сертификата пользователя на основе ГОСТ 34.11.2001. Доступ к контейнеру ключа и сертификата на мобильном устройстве должен быть защищен пин-кодом (не менее 4-х символов).

Шифрованию будут подвергаться следующие данные:

- файлы документов;
- база данных приложения.

Пользователи мобильного приложения смогут производить модификацию документов на устройстве (например, комментирование файлов pdf), а также генерацию документов на мобильном устройстве (результаты голосования по вопросам мероприятия в формате xml). При отправке документов в базу данных при необходимости будет производиться формирование электронной подписи, а на стороне базы данных - ее проверка. Алгоритмы формирования и проверки электронной подписи предлагается реализовать в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Будет реализована нотификация пользователей мобильного кприложения о наличии новых уведомлений (в случае уведомления о предстоящем мероприятии, обновления материалов к мероприятию, переноса срока мероприятия и тп.).

Предлагаемое решение позволит ускорить работу по рассмотрению и согласованию документов, а также улучшит взаимодействие между подразделениями образовательного учреждения.

Жигадло Н.В., Елисеева Е.Н.
Россия, Санкт-Петербург, Гимназия № 652

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ИНТЕРАКТИВНЫХ СРЕДСТВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ В УСЛОВИЯХ ПРЕЕМСТВЕННОСТИ ФГОС НОО

Для выполнения указанной в ФГОС НОО установки на введение в учебный процесс интерактивных способов обучения учителю начальных классов необходимо совершенствовать формы классной работы учащихся. Современный этап развития российского образования характеризуется также широким внедрением в учебный процесс компьютерных технологий, в частности, электронной интерактивной доски (ЭИД). Она позволяет выйти на новый уровень обучения, открывает ранее недоступные возможности, как для учителя, так и для обучающегося. ЭИД представляет собой сенсорный экран, подсоединенный к компьютеру, изображение с которого передается на доску-проектор.

В новых условиях большой интерес представляет рассмотрение двухосновных приемов использования ЭИД в учебном процессе: управление компьютером с ЭИД без использования традиционных клавиатуры и мыши, в основном на организационных моментах урока, при работе с файловой системой компьютера, для запуска приложения Windows, для начала сеанса в сети Интернет и т.д.; совмещение использования электронных заготовок (слайдов, текстов, изображений и др.) с рукописным видом деятельности, позволяя учителю наносить на проецируемое изображение надписи и пометки с помощью электронного маркера поверх электронной заготовки, акцентируя внимание обучающихся на наиболее важной информации, что, может способствовать более качественному освоению изучаемого материала. Каждый чертеж может располагаться на отдельной странице, что позволяет не загромождать доску и не отвлекать внимание обучающихся от решаемой задачи. Существует возможность сохранения заготовок в первозданном виде и их использования при работе с другим классом.

Таким образом, ЭИД содержит огромный потенциал по ее применению в учебном процессе. Использование ЭИД предоставляет учителю и обучающимся уникальное сочетание компьютерных и традиционных методов организации их учебной деятельности. Благодаря техническим возможностям ЭИД можно применять в виде обычной доски (поле для письма маркером), демонстрационного экрана, интерактивного инструмента.

В докладе подробно рассматривается дидактический потенциал использования электронной интерактивной доски в организации учебной деятельности обучающихся. Приводятся наглядные примеры, иллюстрирующие высокую эффективность использования ЭИД на уроках в начальной школе.

Журавлев А.Е.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

СПЕЦИАЛЬНЫЙ ФУНКЦИОНАЛ В ИНФОРМАЦИОННЫХ СИСТЕМАХ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ КОМПЕТЕНЦИЙ В КОНТЕКСТЕ АКТУАЛЬНЫХ ФГОС

Новое поколение федеральных государственных общеобразовательных стандартов (ФГОС), которым положили начало принятые в 2009 году изменения в Закон Российской Федерации «Об образовании», ознаменовало начало одного из важнейших этапов реформы образования. Судить о достигнутых результатах в комплексе пока не представляется возможным, однако, уже сейчас можно с уверенностью заявить, что в связи с введением в оборот новейших положений об образовании необходимо также кардинально пересмотреть и дополнить и фонды оценочных средств. Так, например, ранее для многих современных дисциплин считалось достаточным наличие общих средств автоматизации процесса проверки степени усвоения знаний слушателем. С введением новых ФГОС стали очевидны недостатки такого подхода, и, соответственно, возникла необходимость в разработке и внедрении нового специального функционала для таких информационных систем.

По результатам проведенных в рамках политики общей информатизации процесса обучения исследований стала очевидной потребность в адекватных средствах автоматизированной проверки знаний и умений. Результатом разработки проекта актуализации обучающей информационной системы стал, например, ее специальный модуль форсированной аттестации, включивший в себя подсистемы механизмов блиц-опроса, экспресс-тестирования и динамической адаптации исходящей информации.

В рамках действующей автоматизированной информационно-справочной системы (АИСС) «ВУЗ» и интегрированных внешних компонентов (например, таких, как «Бухгалтерия», «Кадры» и т.п.) было осуществлено внедрение нового специального модуля «Форс». Помимо основного функционала, данный модуль также решает проблемы избыточности накопительной части персонифицированной информации, расширенной поддержки некоторых функций прочих компонентов центральной информационной системы, организации динамического интерфейса с единой системой мониторинга знаний слушателей, выработки индивидуальных рекомендаций слушателям, удаленного доступа к оперативной информации и т.п.

В целом, решение основной проблемы форсированной аттестации признано химерой, что, однако, позволяет успешно решать частный круг задач по оперативной персонификации учебно-тестового комплекса. Так, например, на основании данной подсистему успешно решена задачи мотивации слушателей и их ориентация на достижение максимально возможного результата, в том числе методом многократного повторения изученного материала. Причем, определяющая роль остается именно за слушателем.

Для реализации стратегии оптимального управления имеющимися ресурсами подсистемой предусмотрены внутренние системные интерфейсы для информационной системы принятия решений «Каскад», имеющейся в составе функционирующей АИСС «ВУЗ». Взаимная интеграция информационной системы средствами условно-универсального модуля, обеспечивающего гибкий интерфейс для каждой клиентской компоненты позволяет воплотить в действительности идею единого динамического информационного пространства организации, включающего в себя помимо систем обучения также кадровые, учетно-складские, бухгалтерские и административные компоненты. Единое поле обладает рядом несомненным достоинств, например, общую, всегда актуальную базу данных (БД), позволяющую в реальном времени отслеживать динамику протекающих в АИСС процессов, а также экономить целый пласт ресурсов, обычно затрачиваемых на процессы синхронизации данных отдельными локальными БД; централизацию доступа к сведениям БД, обеспечивающую единый интерфейс для всех категорий пользователей АИСС; унификацию средств обеспечения безопасности при поддержке компоненты «Анализатор», что позволяет максимально оперативно выявить угрозу любому компоненту АИСС и изолировать подвергшийся атаке участок вместе со злоумышленником в специализированной «песочнице» и т.п.

В АИСС «ВУЗ» используется программный коммутатор с функцией шлюза, реализованный на базе интегратора, потому весь его обменный функционал можно рассматривать как модель локальной вычислительной сети и межсетевого взаимодействия. Клиентскими узлами в данной модели выступают объекты работы интегратора, т.е. компоненты, подлежащие организации взаимодействия. Роль сервера и контроллера берет на себя образующая АИСС «ВУЗ». Таким узлом является и рассматриваемая подсистема «Форс».

Функционал шлюза в рассматриваемой модели реализован комплексом генетических алгоритмов, реализующих постулаты теории приближений относительно потоков и каналов передачи данных как объектов мутаций отбора. Коммутатор интегратора реализует систему распределенного хранения и передачи данных путем инициализации авторизированных туннелей класса «коммутатор-узел». В том числе за счет этого, данная сетевая модель во многом наследует идеи семантической модели данных «сущность-связь», не только хранящей объекты данных, но и раскрывающей их смысловое обеспечение и взаимосвязь друг с другом.

Заболотная В.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ БАКАЛАВРОВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА

Государственный образовательный стандарт высшего образования устанавливает достаточно высокие требования к овладению навыками самообучения. Профессиональный рост специалиста, его востребованность как никогда зависят от умения решить нестандартную задачу, от способности к планированию и прогнозированию самостоятельных действий. Стратегическим направлением повышения качества образования в этих условиях является оптимизация системы управления учебной работой обучаемых, в том числе и их внеаудиторной самостоятельной работой (СР).

Электронное обучение является удобным инструментом реализации перечисленных выше задач, дает возможность учета личностных качеств обучаемых, формирует информационную компетентность у бакалавров. Также необходимо отметить, что целесообразно применение электронных технологий и в рамках традиционных форм обучения студентов. Такое их использование способствует интенсификации обучения, требующей перестройки деятельности преподавателя, содержания изучаемого материала, изменения форм организации занятий, использования прогрессивных педагогических технологий обучения. Без применения электронного обучения невозможно осуществить эффективную реализацию ряда требований, приведенных в ФГОС. Например, в государственном образовательном стандарте высшего образования по направлению подготовки «Автоматизация технологических процессов и производств» (квалификация «Бакалавр») содержатся требования к условиям реализации основных образовательных программ бакалавриата, которые могут быть решены при использовании средств электронного обучения.

По результатам наших наблюдений многие студенты приходят в вуз с недостаточным уровнем знаний в области информатики и ИКТ, поэтому они плохо усваивают вузовский курс информатики. Еще одна причина плохой успеваемости студентов первого курса состоит в том, что аудиторные часы на освоение программ многих дисциплин значительно сокращены. Кроме того студенты первого курса, как правило, не умеют планировать свою учебную деятельность, не осознают, что большую часть материала в вузе необходимо изучать самостоятельно. Отметим, что контроль самостоятельной работы часто отсутствует. По этим причинам к концу семестра многие студенты получают низкие оценки, теряют интерес к обучению.

Для перехода к новой системе организации и контроля СРС в вузе должны быть созданы необходимые условия, одно из которых предполагает внедрение в учебный процесс современных образовательных и информационных технологий, в том числе электронных образовательных ресурсов (ЭОР) и электронных учебных курсов (ЭУК).

Нами разрабатывается образовательный ресурс на базе Приднестровского государственного университета им. Т.Г. Шевченко (http://atpp.rfpgu.ru/). Web-ресурс ориентирован на контроль самостоятельной работы бакалавров по направлению «Автоматизация технологических процессов и производств». В рассматриваемом образовательном ресурсе представлена возможность создания преподавателями курсов различной тематики. В каждом курсе может быть несколько разделов, в каждом из разделов может быть от одной до нескольких лекций. Также в каждом разделе присутствует возможность сдачи лабораторной работы (загрузки на сервер для просмотра преподавателем) и обсуждения темы на форуме.

После изучения каждой темы курса представлена возможность тестового контроля знаний учащихся. Система из списка доступных по предмету вопросов формирует для пользователя тест исходя из критериев, которые установлены для курса, это количество вопросов в тесте и количество времени для прохождения тестирования по курсу. Просмотр результатов тестирования студентами представлен в профиле. Также для студентов представлена возможность оперативно связаться с преподавателем для выяснения возникающих вопросов по ходу выполнения задания и получить консультацию у любого преподавателя вуза и раздел, содержащий отчеты с результатами выполнения самостоятельной работы по заданиям. Преподаватель же может просматривать информацию о работе студентов, оценки за выполненные тестовые задания по теме.

В заключение подчеркнем, что в нашем исследовании рассматривается вариант применения электронного обучения в комплексе с традиционными формами проведения занятий по дисциплинам компьютерного цикла. Одним из основных условий повышения эффективности СРС в электронной среде является использование интерактивных методов и технологий, которые будут способствовать активному взаимодействию субъектов учебной деятельности.

Игнатьев М.Б., Попов В.П., Аксенов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

НОВАЯ МАГИСТЕРСКАЯ ПРОГРАММА «КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ»

Предлагается новая образовательная программа по подготовке магистров по киберфизическим системам, которая включает в себя специализированные дисциплины – Теория киберфизических систем, Умные автомобили и дороги, Паттерны Правил дорожного движения и экстремальных ситуаций, Системы ориентации и навигации подвижных объектоа, Проблемы понимания экстремальных ситуаций.

Программа базируется на взаимодействии с семью филиалами крупных автомобильных компаний – Форд, Тойота и др

Камерис А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ МУЗЫКАЛЬНО-КОМПЬЮТЕРНОГО ОБРАЗОВАНИЯ В СИСТЕМЕ ПОДГОТОВКИ ПЕДАГОГА-МУЗЫКАНТА

Начало XXI века ознаменовалось внедрением компьютерных и коммуникационных технологий во все сферы человеческой деятельности. Глобальные изменения произошли в способе передачи информации и в ее представлении.

Цифровые технологии проникли в музыкальное творчество и образование. Достижения звукозаписи, технологии создания музыкальных композиций в сочетании с новыми возможностями средств массовой информации определили несуществовавшие ранее области развития и распространения музыки, и требуют таких знаний, которыми музыканты, получившие академическое музыкальное образование, не обладают.

Разработка нового подхода к высшему, среднему профессиональному музыкальному образованию обусловлена необходимостью решения острейших проблем в массовой музыкальной педагогике. Так, на конференциях “Современное музыкальное образование”, организованной совместно РГПУ им. А.И. Герцена и СПб консерваторией им. Н.А. Римского-Корсакова, музыковеды, преподаватели музыкальных дисциплин отмечали, что несмотря на выдающиеся творческие достижения, возможности музыкального образования в массовой педагогике используются не полностью, методы обучения в системе общего музыкального образования существенно не изменяются.

Один из путей решения этой проблемы заключен в поиске новых педагогических технологий. Их необходимо совершенствовать и создавать музыкальные программы, которые позволили бы гибко и разносторонне использовать богатый педагогический инструментарий в обучении музыке и огромные возможности музыкального компьютера (МК). Однако в новой сфере существует ряд проблем. Т

ак, многие учебные заведения не всегда успевают следить за быстро меняющимся миром цифровых технологий. Возникает необходимость создавать мобильные образовательные системы, способные быстро адаптироваться к изменяющейся информационно-коммуникационной среде. Встает проблема подготовки специалистов, соответствующих современному требованию музыкального образования.

В системе профессионального развития педагогов-музыкантов одним из важнейших является процесс информатизации образования. Сегодня для решения этой задачи все шире начинает использоваться Интернет. Появляется больше возможностей, связанных с использованием современных технологий. Сформировано сетевое профессиональное педагогическое сообщество преподавателей, которое позволяет им общаться между собой, не выходя из образовательного учреждения.

Музыкально-компьютерные технологии (МКТ), динамично развиваясь, определили возможность создания новой профессионально-образовательной творческой среды.

Дидактические аспекты проблемы компьютеризации музыкального обучения в России разрабатывали ученые и педагоги Ю.Н. Рагс, И.Б. Горбунова, Н.С. Сушкевич, Н.А. Терентьева, И.М. Красильников, Е.В. Орлова, Р.Х. Зарипов, П.Л. Живайкин, Э. Мансфельдерс, С.П. Полозов, М.В. Карасева и др. По данному направлению опубликованы научные статьи и монографии, методические и учебные пособия, программы и нотные сборники для учащихся.

Тем не менее, несмотря на востребованность информационных технологий в музыкальной практике и разработку ряда вопросов теории тема остается «открытой». Недостаточно внимания уделяется внедрению МКТ в систему образования, поэтому требуется серьезное научное обобщение сделанного в данной области.

В этой связи исключительно ценен опыт РГПУ им. А.И. Герцена, где создана новая концепция музыкально-компьютерного педагогического образования. Она заключается в разработке высшего музыкального педагогического образования на базе МКТ (бакалавриат, магистратура) под

руководством И.Б. Горбуновой – председателя УМК МКТ в художественном образовании (профиль и магистратура «Музыкально-компьютерные технологии в образовании»), а также программы профессиональной переподготовки – «Преподавание музыкальных дисциплин с использованием музыкально-компьютерных технологий» и программ повышения квалификации.Изложению основных идей данной концепции посвящен доклад.

Касаткин В.В., Советов Б.Я.
Россия,Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНТЕГРАЦИЯ ОБРАЗОВАНИЯ, НАУКИ И ПРОМЫШЛЕННОСТИ КАК ОСНОВА РОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ ИТ-СПЕЦИАЛИСТОВ ПРИ МНОГОУРОВНЕВОЙ ПОДГОТОВКЕ

В условиях отсутствия уровня инженерной подготовки кадров по направлению «Информационные системы и технологии», входящего в укрупненную группу специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника», особую остроту приобретает проблема быстрой адаптации выпускников – разработчиков информационных систем и технологий к выполнению трудовых функций в условиях производства.

В структуру актуализированных федеральных государственных образовательных стандартов включены отдельные требования работодателей, однако реализация этих требований вузом зачастую затруднена ввиду резкого снижения объема научных исследований, сложности организации производственной практики, а также вынужденного (в соответствии с указаниями Минобрнауки) руководства выпускными квалификационными работами лишь со стороны преподавателей вуза.

В связи с этим особую актуальность приобретает развитие существующих форм интеграции науки, образования и промышленности.

Наряду с уже сложившимся связями в виде учебно-производственных комплексов, малых научно-производственных предприятий при вузах, базовых кафедр, учебно-образовательных лабораторий всвязи с недостаточностью финансирования, как внутреннего, так и внешнего, вузы вынуждены обращаться к таким формам, как соглашения о сотрудничестве с крупными корпорациями и зарубежными университетами, что зачастую экономически не поддерживается ни со стороны государства, ни со стороны партнеров. В этих условиях необходимым условием решения проблемы является изменение государственной политики в направлении обеспечения заинтересованности со стороны промышленности выделения гарантированных рабочих мест в формах, сходных с существовавшим ранее распределением выпускников вузов.

Это позволило бы, исходя из требований работодателя, с учетом региональных потребностей рынка труда формировать контрольные цифры приема вуза на обучение за счет бюджетных средств, ориентируя высшую школу на реальные потребности работодателей и возможности трудоустройства выпускников.

В современных экономических условиях применительно к области информационных технологий это предложение может быть наиболее эффективно реализовано при условии восстановлении уровня специалитета в структуре наиболее востребованных со стороны предприятий реальных секторов экономики, (в первую очередь, – высокотехнологичных отраслей промышленности) направлений подготовки кадров, связанных с разработкой, применением и внедрением аппаратных и программных средств ИКТ, в значительной степени ориентированных на реализацию программ импортозамещения. В этом отношении приоритетным является переход от стратегии импортозамещения к стратегии импортоопережения, для чего необходимо на младших курсах сфокусировать внимание на обеспечение фундаментальности обучения, а на старших –на реализацию практико-ориентированной подготовки.

Сложность решения указанной задачи состоит в обеспечении условий, при которых предприятия проявляли бы заинтересованность и осознавали ответственность за обеспечение гарантий трудоустройства выпускников вузов и качество подготовки кадров, что, в конечном счете, позволило бы повысить уровень трудоустройства выпускников по специальности и сократить непроизводительные затраты предприятий на профессиональную переподготовку и повышение квалификации молодых специалистов.

В качестве положительного опыта следует признать реализацию предложения о включении в структуру укрупненной группы специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника» основной образовательной программы специалитета по направлению «Применение и эксплуатация автоматизированных систем специального назначения», разработанной на основе использования многолетнего опыта разработчиков трех поколений федеральных государственных образовательных стандартов инженерной подготовки кадров в области техники и технологий.

Касаткин В.В., Советов Б.Я., Яковлев С.А.
Россия,Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

АКТУАЛИЗАЦИЯ ПРИМЕРНЫХ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ НА ОСНОВЕ СОПРЯЖЕНИЯ ФГОС С ПРОФЕССИОНАЛЬНЫМИ СТАНДАРТАМИ

Сложившаяся в настоящее время многоуровневая система подготовки кадров в высшей школе не согласуется в достаточной мере с реальными потребностями работодателя, что приводит к невостребованности выпускников вузов. Более половины выпускников вынуждены устраиваться на работу не по специальности. Это связано с тем, что принятая в Российской высшей школе модель бакалавра не ориентирована на быструю адаптацию выпускника на рабочем месте, т.е. наблюдается недостаточность его профессиональной подготовки. Работодатель не считает выпускника сложившимся специалистом, что влечет за собой необходимость совершенствования содержания подготовки и, в первую очередь, - необходимость актуализации федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) в части сопряжения и максимального приближения их к профессиональным стандартам (ПС).

Ключевыми аспектами применения ПС в процессе актуализации ФГОС ВО и разработки примерных образовательных программ следует считать: обеспечение соответствия квалификационных уровней и содержания обобщённых трудовых функций в утвержденных ПС; обобщение опыта применения ПС при разработке и актуализации ФГОС ВО; повышение качества утверждаемых ПС в части установления требований к профессиональной квалификации работника; непрерывное совершенствование ФГОС ВО, актуализируемых с утверждаемыми ПС; удовлетворение потребностей работодателей, снижение неоправданных затрат работодателей на переобучение, дополнительное образование выпускников, поступающих на работу; совершенствование системы профессиональных квалификаций в конкретных областях профессиональной деятельности на общероссийском уровне.

Учебно-методическим советом по направлению «Информационные системы и технологии» была проведена работа по актуализации ФГОС ВО по направлениям подготовки 09.03.02, 09.04.02 в части: определения перечней ПС, сопрягаемых с соответствующими ФГОС ВО; учета положений ПС из указанных перечней; определения совокупности обобщенных трудовых функций, соответствующих выбранным ПС; внесения в ФГОС ВО указания на ориентацию соответствующей основной образовательной программы на освоение конкретных обобщенных трудовых функций; внесения требований к обеспечению качества образования.

В перечень ПС, сопрягаемых с указанными ФГОС ВО, включены следующие ПС: Программист; Архитектор программного обеспечения; Специалист по тестированию в области информационных технологий; Администратор баз данных; Специалист по информационным ресурсам; Менеджер по информационным технологиям; Специалист по информационным системам; Руководитель проектов в области информационных технологий; Руководитель разработки программного обеспечения; Технический писатель (специалист по технической документации в области информационных технологий); Системный аналитик.

К обобщенным трудовым функциям, сопрягаемым с ФГОС ВО «Информационные системы и технологии» отнесены: разработка требований и проектирование программного обеспечения; оценка возможности создания архитектурного проекта; утверждение и контроль методов и способов взаимодействия программного средства со своим окружением; модернизация программного средства и его окружения; разработка документов для тестирования и анализ качества покрытия; разработка стратегии тестирования и управление процессом тестирования; обеспечение информационной безопасности на уровне баз данных; управление (менеджмент) информационными ресурсами; управление ресурсами информационных технологий; выполнение работ и управление работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы; управление проектами в области информационных технологий на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров; непосредственное руководство процессами разработки программного обеспечения; организация процессов разработки программного обеспечения; разработка технических документов, адресованных специалисту по информационным технологиям; руководство рабочей группой технических писателей (специалистов по технической документации в области информационных технологий); концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности.

Позднее в сформированный перечень были добавлены следующие ПС: Разработчик Web и мультимедийных приложений; Специалист по большим данным; Специалист по интернет-маркетингу; Специалист по интеграции облачных приложений.

Результаты актуализации ФГОС ВО и разработки примерных образовательных программ должны позволить работодателю четко определить рабочие места для выпускников бакалавриата и магистратуры по направлению «Информационные системы и технологии», а также сориентировать вузы на реализацию требований мониторинга с целью повышения качества подготовки кадров.

Касаткин В.В., Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современной модели образования подчеркивается, что необходимым условием формирования инновационной экономики является модернизация системы образования, становящейся основой динамичного экономического роста и социального развития общества, фактором благополучия граждан и безопасности страны. В связи с этим в сфере высшего образования исследуются проблемы обновления содержания инженерного образования, определяется роль современных технологий обучения в системе средств повышения его качества. В подготовке ИТ-специалистов технического профиля в вузе все большее признание получает технология имитационного моделирования.

В настоящее время в игровом имитационном моделировании широко представлены: деловые игры (производственные, исследовательские, военные, учебные т.д.); аттестационные игры для подбора и назначения кадров, для оценки уровня их квалификации; ситуативно-ролевые игры; производственные деловые игры; исследовательские деловые игры; учебные деловые игры и т.д.

Однако имитационное моделирование как технология подготовки ИТ-специалистов технического профиля до настоящего времени не было подвергнуто специальному анализу, в частности, учитывающему следующие противоречия:

- между возросшими требованиями государства к ИТ-специалисту, конкурентоспособному на рынке труда, и недостаточно адекватной профессиональной и личностной подготовкой выпускников вузов к выполнению своих профессиональных функций в новых социальных условиях;
- между многообразием концептуальных подходов к проблеме технологий образования и недостаточной разработанностью имитационного моделирования как технологии подготовки специалистов технического профиля в вузе.

В связи с социально-педагогической значимостью проблемы профессиональной подготовки современных ИТ-специалистов технического профиля и выявленными противоречиями была определена тема исследования, целью которого является разработка научно-методических основ использования технологии имитационного моделирования в подготовке ИТ-специалистов технического профиля в вузе.

Объектом исследования выступает технология имитационного моделирования в подготовке ИТ-специалистов в высшем учебном заведении, а предметом исследования - организационно-методическая система имитационного моделирования как технология профессиональной подготовки будущих IT-специалистов технического профиля.

Исходя из цели исследования, были определены и решены следующие задачи:

1. Проведен теоретический анализ технологии имитационного моделирования и раскрыты особенности ее использования в процессе подготовки ИТ-специалистов технического профиля в вузе;
2. Обоснована технология имитационного моделирования как средство формирования профессиональной компетентности ИТ-специалистов технического профиля;
3. Разработана методика использования технологии имитационного моделирования в образовательном процессе технического университета.

Исследование проводилось в три этапа, что что нашло отражение в структуре разработанной методики.

Проблемно-поисковый этап. Изучение проблемы высшего технического образования, практики использования современных технологий обучения в вузе, технологии имитационного моделирования. Определение проблемы и темы исследования, его методологических и теоретических основ.

Опытно-экспериментальный этап. Разработка технологии имитационного моделирования применительно к обучению студентов технических специальностей. Анализ и обработка полученных данных

Аналитико-обобщающий этап. Теоретическое осмысление полученных результатов. Мониторинг качества подготовки студентов технических специальностей с использованием технологии имитационного моделирования. Разработка и внедрение в практику рекомендаций по использованию технологии имитационного моделирования в образовательном процессе технического университета.

Внедрение и апробация предложенной методики проводилась при проведении практических занятий, лабораторных работ и курсового проектирования со студентами бакалавриата и магистратуры направления подготовки «Информационные системы и технологии» при реализации федерального государственного образовательного стандарта третьего поколения, а также при разработке версии 3++, актуализированной с соответствующими профессиональными стандартами.

Каткова И.В., Павлова С.М.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

В настоящее время современный период развития общества характеризуется сильным влиянием на него компьютерных технологий, которые проникают во все сферы человеческой деятельности, обеспечивают распространение информационных потоков в обществе, образуя глобальное информационное пространство. Поэтому неотъемлемой и важной частью является компьютеризация образования. В настоящее время в России идет становление новой системы образования, ориентированного на вхождение в мировое информационно-образовательное пространство.

Экономика современной России вступила в стадию постиндустриального развития. Важным фактором социально-экономического развития в постиндустриальном обществе является постоянно обновляемое знание. В современных условиях одной из основных задач образования состоит в его способности порождать спрос на новые знания. Поэтому образовательный процесс в современных условиях должен быть непрерывным. Таким образом, формирование системы непрерывного образования обусловлено необходимостью обеспечения устойчивого социально-экономического развития современного российского общества и более полного удовлетворения потребностей в образовании широких слоев населения.

По мнению авторов Лиссабонской декларации, к основным принципам информационных технологий непрерывного образования можно отнести:

– развитие новых базовых знаний и навыков для всего населения страны, всем гарантируется всеобщий непрерывный доступ к образованию с целью получения и обновления знаний и навыков, необходимых для включение работающих в информационное общество. Социально-экономические перемены в обществе требуют нового набора необходимых базовых знаний, умений и навыков, которые обеспечивали бы членам общества активное участие в профессиональной, семейной и общественной жизни. К ним следуют отнести:

– компьютерную грамотность, иностранные языки, технологическую культуру, предпринимательство, социальные навыки и др.

– инновационные методики преподавания и учения, основная цель которых заключается в разработке новых методических методов обучения для системы непрерывного образования;

– развитие наставничества и консультирования для обеспечения каждому члену общества свободного доступа к информации об образовательных возможностях в своей и в других странах, к необходимым консультациям и рекомендациям;

– приближение образования к дому с помощью сети учебных и консультационных пунктов, а также с помощью информационных технологий, что предполагает создание культурно-просветительских центров в непосредственной близости не только в школах и вузах, но и в торговых центрах, клубах, музеях, библиотеках, религиозных центрах, парках, центрах отдыха и на рабочих местах.

Вышеуказанная информация показывает нам, что система высшего образования страны обладает мощным научно-техническим потенциалом, способным решать важные народно-хозяйственные проблемы инновационного развития экономики.

Для успешной интеграции России в общеевропейское образовательное пространство и занятия достойного места на внутреннем и международном рынках образовательных услуг необходимо проведение последовательной государственной политики, направленной на повышение качества всех уровней образования.

В любом обществе развитие высшего образования тесно связано с динамикой социально-экономического развития самого общества, ибо оно является частью последнего. Запросы общества к образованию постоянно растут и видоизменяются, что проявляется в необходимости постоянной его модернизации и в обновлении. В настоящее время общество ожидает от образования перемен по адаптации его к глобализации и технологическим изменениям, приобретающим характер смены технологического уклада.

Решение этих задач требует комплексных усилий не только школы, вуза но и всего общества. Он становится непрерывным. Система непрерывного образования не декларация, а насущная потребность каждого человека. Поэтому уже в настоящее время возникла необходимость не только в очном обучении, но и в дистанционном, на основе современных информационных технологий. Построение единого информационного пространства в образовании позволит добиться: повышение

эффективности и качества процесса обучения; интенсификации процесса научных исследований в образовательных учреждениях; сокращение времени и улучшения условий для дополнительного образования и образования взрослых; интеграции национальных информационных образовательных систем в мировую сеть, что значительно облегчит доступ к международным информационным ресурсам в области образования, науки, культуры и в других сферах.

Кибиткина Э.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

МЕТАМЕТОДИЧЕСКИЕ ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МУЛЬТИМЕДИА

Подготовка специалистов в области информационных технологий в мультимедиа подразумевает формирование у обучаемых профессиональных компетенций в двух значительно отличающихся друг от друга областях: информатики – точной науки и мультимедийного искусства – творческой сферы. Следовательно, для достижения большей результативности подготовки целесообразно организовать образовательный процесс на метаметодических основаниях, учитывающих и выстраивающих в единую систему все элементы методики обучения и способствующих становлению обучающихся как творческих личностей и профессионалов с системным взглядом на мультимедиа. Основные особенности подобного подхода к образовательному процессу следующие.

Во-первых, необходимо провести логические параллели в содержании обучения с целью формирования единой картины мира, выделяя межпредметные понятия (такие как функция, программа, система, исполнитель, звук, свет, спектр, композиция, гармония, образ), выбирая наиболее важные из них и затем структурируя на их взаимоотношениях всё содержание обучения (последовательности разделов дисциплин и сами дисциплины).

Например, звук имеет существенно отличающиеся определения по крайней мере в четырёх широких областях знания:

- в физике (и акустике) – как физический объект; наиболее "базовое" определение, поскольку требует лишь наличия объективного источника и среды; изучается первым, вместе с физико-математическими курсами;
- в психофизиологии (биологии) – как субъективное (а) ощущение или (б) воспоминание; требует наличия субъективного приёмника и некоторой подсознательной интерпретации; изучается вторым, наряду с естественнонаучными дисциплинами
- в информатике – как форма существования информации; подразумевает представление данных в самых разнообразных формах, но не требует сложного субъективного и философского анализа; изучается третьим вместе с курсами по информатике и ИТ;
- в искусстве (психологии, культурологии, музыкознании) – как основное средство художественной выразительности в музыке; подразумевает неоднозначность и субъективность; изучается четвёртым, параллельно с гуманитарными курсами (философией, культурологией и т.п.) и проектированием интеллектуальных систем.

Практически идентично звуку по областям применения понятие свет, следовательно, изучаться звук и свет могут параллельно, окончательно объединяясь на пятом этапе – в ходе освоения мультимедийного искусства, в котором слуховой и визуальный образы вместе позволяют добиться системного, синергетического эффекта. На этом этапе обучаемые нуждаются в курсах, обобщающих имеющиеся знания и умения, объединяющих их методологически: режиссуре, драматургии, основам проектной деятельности, а также связанных с реализацией творческих проектов в реальной социально-экономической действительности (менеджмент, экономика).

Во-вторых, для реализации метаметодического подхода, целесообразно выделить общее в методах, формах и средствах обучения техническим и творческим дисциплинам, подчинить их логике развития содержания.

Дисциплины, связанные с информатикой, можно преобразовать в более значимые и полезные для обучаемых, если решаемые на занятиях и самостоятельно задачи непосредственно связаны с мультимедиа. Также можно расширить спектр методов обучения, включив в их число более творческие. Творческие дисциплины наполнить методологией точных наук, обращать внимание обучаемых на "дуалистичную" природу современного искусства, объединяющего в себе программирование (конкретику, предопределённость) и творческий подход (интуитивность, многозначность), на необходимость учёта её достоинств и ограничений.

Таким образом, по окончании образовательного процесса, построенного по указанным принципам, мы можем получить компетентных специалистов, осознающих всю многогранность мультимедийного творчества, владеющих широким спектром информационных технологий и умеющих осознанно и эффективно выбирать средства реализации художественных задач, соответствующие конкретной ситуации, и гармонично сочетающих в себе техническое и гуманитарное мировоззрение.

Климов А.Н., Терехин Д.В., Чирушкин К.А
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРЕДПОСЫЛКИ И АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ УЧЕБНЫХ ТРЕНАЖЕРОВ В ПРОЦЕССЕ ПОДГОТОВКИ КАДРОВ И КОНТРОЛЯ НАВЫКОВ ПРИ ВЫПОЛНЕНИИ РАБОТ НА ВЫСОКОТЕХНОЛГИЧНОМ ОБОРУДОВАНИИ

С бурным развитием компьютерных технологий появилась возможность моделировать сложные технологические комплексы для подготовки и повышения квалификации специалистов в различных областях человеческой деятельности. На фоне реформирования, перевооружения и бурного развития Вооруженных сил Российской Федерации, данный аспект получил широкое распространение в процессе обучения «воинов-связистов». В связи с технологической сложностью и высокой стоимостью создания оборудования, а соответственно высоким уровнем амортизационных затрат одним из целесообразных решений на данном этапе является использование учебных тренажеров. Однако, в настоящее время нет единого подхода и четкого регулирования на законодательной основе порядка использования или методологии создания для вооруженных сил и подразделений связи в частности. Таким образом ярким примером может служить опыт зарубежных партнеров, при использовании компьютерных тренажеров (автоматизированных систем обучения – АСО) для обучения персонала в нефтегазодобыче, переработке и нефтехимии который становится законодательной нормой. Так в США федеральный стандарт предписывает обязательный компьютерный тренинг для всех принимаемых на работу операторов и тренажерный курс переподготовки для всех действующих операторов не реже одного раза в три года.

Внутренние правила ведущих нефтяных компаний мира предполагают обязательный восстановительный курс после отпусков, болезни или длительного отсутствия практики по другим причинам. В РФ действующие «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (ПБ 09-540-03), пункт 2.12 гласят, что для приобретения навыков безопасного ведения работ все операторы производств I и II категории должны пройти курс обучения на компьютерных тренажерах, в основе которых лежат динамические модели. Такие меры приняты для безопасного ведения процесса и предотвращения аварийных ситуаций.

Использование имитационных тренажерных комплексов позволяет повысить профессиональный уровень, дать необходимый практический опыт – отрабатывать базовые навыки работы с системой управления и навыки действий в аварийных ситуациях без риска повлиять на ход реального технологического процесса и не прибегая к экспериментам на реальных объектах.

Одним из перспективных направлений развития в данной области является создание виртуальных тренажеров. Основная задача таких тренажеров – формирование комплексного навыка принятия решений, который основывается на возможности смоделировать динамический отклик объекта и системы управления на произвольные управляющие воздействия оператора. Т.е. по сути, тренажеры являются теми же программами моделирования процессов в динамическом режиме с обязательным требованием обеспечения режима реального времени.

Таким образом при создании виртуального тренажера разработчик применяет методы имитационного моделирования и выполняет ряд рабочих этапов:

- разработка математических моделей, имитирующих процессы, протекающие в моделируемой системе;
- реализацию указанных моделей в режиме имитации (или динамического моделирования);
- воссоздание рабочего места оператора, подобного рабочему месту в реальном процессе, включая организацию операторского интерфейса и органов управления;
- разработку методов анализа и оценки результатов тренинга, методов аккредитации операторов по результатам обучения на тренажерах.

Использование виртуальных тренажеров позволяет устранить ещё один недостаток традиционного способа обучения – это отдельное проведение лекционных и лабораторных работ.

Виртуальная реальность – идеальная обучающая среда. Восприятие виртуальной модели с высокой степенью достоверности позволяет качественно и быстро готовить специалистов в различных областях.

Виртуальные тренажеры в процессе военно-профессионального обучения, с учетом имеющихся требований по овладению набором необходимых знаний и навыков, могут иметь практическое приложение и использоваться в целях определения наличия соответствующих компетенций военных профессионалов, а также для определения классной квалификации специалистов. Постоянное применение тренажеров способствует поддержанию подготовки специалистов на должном уровне и способствует своевременному выявлению необходимости в обучении.

Колоколова Л.П.
Россия, г. Стерлитамак, Стерлитамакский филиал Башкирского государственного университета

ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА ПРИ ИЗУЧЕНИИ КОРПУСНОЙ ЛИНГВИСТИКИ

В настоящее время существует довольно большое число языковых корпусов, которые отличаются друг от друга по самым разным параметрам, поэтому в учебном процессе наблюдается устойчивый интерес исследователей к привлечению информационных технологий в преподавание корпусной лингвистики. Внедрение информационных технологий (ИТ) в образовательный процесс не столько насущная необходимость, сколько осознанный процесс технологизации рутинных процессов с целью проведения лингвистического анализа компьютеризированных текстовых корпусов. Информационные технологии в обучении русскому языку позволяют интегрировать в рамках одной программы тексты, графику, звук, высококачественные фотоизображения.

Таким образом, одной из наиболее важных задач, стоящих перед российской системой образования, является обеспечение доступности и качества образовательного процесса, итогом которого должно быть формирование конкурентоспособного выпускника. Данная цель не может быть достигнута без широкого внедрения, без опоры на современные информационные технологии в образовании.

В рамках корпусной лингвистики информационные технологии позволяют решить следующие задачи: сформировать в сознании специалистов гуманитарного профиля необходимые для научной и педагогической деятельности базовые представления о корпусной лингвистике; представить полученные ранее знания о языке, тексте и коммуникации с точки зрения корпусной лингвистики; освоить новейшие технологии быстрого получения необходимого материала при учёте правильного формирования пользовательского запроса.

Методологически внедрение ИК в процесс обучения ускоряет передачу и освоение знаний и способствует формированию языковых корпусов. Важным качеством современных ИТ является их универсальность: они могут быть основой в организации любой деятельности, связанной информационным обменом, основой в создании общего информационного языкового пространства.

Наибольшую популярность среди технических приложений лингвистики получило компьютерное обучение. Компьютер является многофункциональным помощником, хорошим методическим инструментом наряду с другими средствами обучения. Актуальность компьютерных технологий в преподавании русской словесности налицо, так как новые условия, непринужденная обстановка, общение с компьютером, одобрение электронного помощника результатов труда имеют позитивную оценку. Студенты с разной степенью грамотности сосредотачиваются на ключевых моментах, так как машина идет вместе со студентом от незнания к знанию, акцентируя внимание на неусвоенном материале. Компьютерное обучение даёт возможность представить разные типы корпусов: Брауновский корпус, Ланкастерско-Ссло-Бергенский корпус (LOB), Бирмингемский корпус, Британский национальный корпус, Национальный корпус русского языка, Хельсинкский аннотированный корпус русского языка, Словацкий национальный корпус, Хорватский национальный корпус и др.

Информационные технологии позволяют представить в объёме национальный корпус, его размер, хронологический охват языка, репрезентативность корпуса, филологическую экспертизу, типы аннотирования, а также метаразметку как часть поискового аппарата корпуса, различные технологии разметки (автоматическая, полуавтоматическая ручная разметка).

Технические средства успешно находят применение при составлении словарей, созданных на базе корпуса (традиционные словари, электронные словари, частотные словари разного типа: с входной единицей – лексемой, с входной единицей – словоформой; частотный словарь словоформ русского языка). Например, по теме «Лексикография» важно учитывать следующие этапы работы: 1) предмет, объект, задачи изучаемой проблемы, 2) словарь, структура словаря, 3) понятие словарной статьи, структура словарной статьи, 4) функции словарей, 5) типология словарей, 6) лексикографический анализ слова. Технические средства дают возможность представить исследовательскую работу в целом и затем поэтапно рассматривать каждый отдельный информационный блок. Особенно этот вид деятельности характерен при анализе схемы комплексного лексикографического анализа, включающего следующие виды деятельности: 1) дать полное название словаря, 2) указать, выходные данные (автор (ы), год издания, место издания, издательство), 3) определить объект описания, 4) охарактеризовать структуру словарных статей и их содержание, 5) определить принцип построения словаря, 6) определить структуру словаря, 7) определить, на кого рассчитан словарь, 8) охарактеризовать объём словаря и специфику его оформления: таблицы, схемы, карты, иллюстрации, фото ит.п., 9) описать словарную статью.

Совершенно очевидно, что информационные технологии (ИТ) – это широкий спектр цифровых технологий, используемых для создания, передачи и распространения информации и оказания услуг (компьютерное оборудование, программное обеспечение, телефонные линии, сотовая связь,

электронная почта, сотовые и спутниковые технологии, сети беспроводной и кабельной связи, мультимедийные средства.

Примером успешной реализации ИКТ в современном учебном процессе стало появление Интернета – всемирной компьютерной передачи с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю. Технология Интернет как среда коммуникации является посредником во включении студента в сетевые структуры, на основе которого он получает возможность эффективно использовать информацию, предоставляя ее заинтересованным людям в кратчайшие сроки.

Совершенно очевидно, в рамках дисциплины «Корпусная лингвистика» эффективность обучения может быть значительно повышена с помощью ИТ, применяемых в различных оптимальных для данных занятий сочетаниях с другими средствами обучения.

Комарова С.М.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена

ОБУЧЕНИЕ СТУДЕНТОВ КОМПЬЮТЕРНОМУ МОДЕЛИРОВАНИЮ НА ОСНОВЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ

Роль математического и компьютерного моделирования в процессе вузовской подготовки на современном этапе развития общества возрастает, особенно для направлений, связанных с математикой и информационными технологиями, в том числе и педагогических соответствующего профиля. Это связано с тем, что любая деятельность по проектированию не возможна без процесса моделирования. Таким образом, весьма актуальной представляется разработка нового подхода к обучению студентов математическому и компьютерному моделированию, ориентированного на:

- компетентностный подход, выполнение требований федерального государственного образовательного стандарта высшего образования;
- реализацию межпредметных связей информатики и математики, которая выражается в использовании математических методов, средств информационных технологий, в частности средств программирования, для построения и исследования компьютерных моделей;
- системный принцип отбора содержания обучения моделированию, при котором методы математического и компьютерного моделирования изучаются студентами одновременно с основами программирования;
- практическую направленность задач компьютерного моделирования, являющихся значимыми в соответствующей предметной области

Моделировать элементы будущей профессиональной деятельности специалиста позволяет метод проектов.

При обучении студентов компьютерному моделированию метод проектов целесообразно применять, т.к. он обладает рядом преимуществ по сравнению с другими методами обучения: способствует развитию способности самостоятельно находить информацию, необходимую для решения задачи, готовности построить и исследовать компьютерную модель в соответствии с условием задачи, предложить пути ее совершенствования, способности к самообразованию, самосовершенствованию, результатом проектной деятельности в области компьютерного моделирования является приложение, созданное в среде программирования, т.е. «осязаемый» продукт и т.д.

Мини-проекты, созданные студентами в процессе обучения в среде объектно-ориентированного программирования, позволяют оценить уровень достижения ожидаемых результатов обучения, которые мы соотносим с категориями таксономии педагогических целей Б. Блума, в особенности ожидаемые результаты, относящиеся к категориям анализа, синтеза и оценки, которые являются наиболее сложными для усвоения у студентов.

Разработанный автором подход к обучению компьютерному моделированию студентов бакалавриата педагогических направлений подготовки, специализирующихся в области информационных технологий прошел апробацию в РГПУ им. А.И. Герцена, результаты которой свидетельствуют о целесообразности использования метода проектов для развития у студентов готовности применять компьютерное моделирование в профессиональной деятельности при решении практических задач.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

СОЦИАЛЬНЫЕ СЕТИ И ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС

Сегодня создание социальной среды в вузе, мотивирующей сотрудников и студентов на постоянный рост собственных знаний и постоянное совершенствование процессов получения и закрепления новых знаний, является необходимым условием процветания.

В настоящее время в государственных и корпоративных, гражданских, научных, тематических и профессиональных сообществах приобрели популярность различные формы сетевого общения с использованием ИКТ, которые применяются в различных областях деятельности организаций, таких, как распространение информации внутри компании, коллективная разработка проектов, связи с клиентами, управление контентом, маркетинг и PR, а также в управлении знаниями.

Применительно к вузам основными процессами, где происходит извлечение, накопление и распространение знаний являются учебный процесс, научные исследования и разработки, материализация и коммерциализация результатов НИР и НИОКР, разработка учебных материалов.

Современный вуз по своему годовому финансовому обороту, по размерам, по объему и стоимости основных средств, по структуре ничем не отличается от крупных предприятий производства или сферы услуг.

Применительно к вузам изменяются роли различных форм сетевого общения при управлении знаниями, которые позволяют:

– создавать книги и научные работы, каталоги ошибок и трудностей по проектам и направлениям, инструкции по процессам и программному обеспечению с реальными практическими примерами пользователей, документацию по процессам; при e-leaning позволяют создавать простые электронные курсы с комментариями слушателей, организовывать коллективную работу слушателей, базу ресурсов и документов по тематике обучения.

– организовывать совместную работу над проектами, обсуждение проблем сотрудниками разного уровня и из разных регионов, мониторинг нового в отрасли, отслеживание интересов и профессионального развития сотрудников; при e-leaning позволяют обеспечивать обучение на основе свежих ресурсов и формирование мнения о происходящем в обществе, работу группы над проектом в процессе обучения, подборку источников и построение взаимосвязи между ними, самостоятельную работу слушателей.

– создавать информацию о новых инструкциях и документах, рассылку новостей, рассылку вопросов сотрудников и проблем проектов, запись трансляций выступлений руководителей, сотрудников, организовывать асинхронные аудио-конференции; при e-leaning позволяют создавать информацию о новостях курса или программы, информацию о новых курсах, новых возможностях обучения, подписку на полезные для курса источники, вопросы слушателей, аудио-лекции, организовывать использование информации в свободном доступе для обучения.

Социальную сеть можно определить как социальную структуру, объединяющую отдельных людей или даже целые организации.

Социальная сеть показывает, каким образом ее участники связаны друг с другом теми или иными отношениями — от случайных знакомств до тесных семейных связей.

В ВУЗе объектами внимания должны становиться разномасштабные группы людей, причем в первую очередь такими объектами должны быть учебные группы студентов.

В структуре взаимоотношений данной группы желательно наличие преподавателей, включенных внутрь сетевого общения.

Важно соблюдать баланс между слабыми и сильными связями в социальных сетях — первые дают дополнительные источники инноваций, а вторые помогают создавать и поддерживать необходимый рабочий микроклимат.

Социальные сети могут выявить неформальные связи между участниками группы, что может оказаться полезным в организации образовательного процесса.

Социальные сети помогают наводить мосты между иерархической организационной структурой ВУЗа и неформальной горизонтальной структурой социальных связей для достижения стратегических целей обучения.

ВУЗ объединяет людей, которые заинтересованы в приобретении и развитии знаний в определенной области, их использовании на практике и для достижения таких целей постоянно взаимодействуют друг с другом.

А технологии, системы и структуры накопления и доступа к информации, такие как внутривузовские компьютерные сети, порталы и программные продукты совместной работы, обеспечивают инструментальную поддержку управления знаниями.

Для идентификации социальных сетей с целью последующего анализа используются, как правило, интервью, опросы, специальные методы наблюдений. Множатся сайты, поддерживающие виртуальные сообщества.

В докладе рассматриваются вопросы влияния использования социальных сетей, основанных на современных информационных технологиях, на организацию процесса обучения. Приведены наиболее яркие примеры их включения в образовательный процесс.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС И ИКТ

Для успешного социально-экономического развития страны, а также развития и успешной жизнедеятельности личности необходимо иметь соответствующий уровень образованности граждан.

Сегодня современные образовательные институты должны способствовать расширению адаптационных возможностей личности в части ее способности и готовности менять сферы и способы деятельности. Тем самым, система образования должна не просто хорошо учить, но, что очень важно, прививать навыки самообучения и воспитывать готовность учиться в течение всей жизни, обучать личность получать удовольствие от процессов познания и творчества, развивать способность взаимодействия с другими людьми.

Активное внедрение в учебный процесс информационно-коммуникационных технологий (ИКТ) требует глубоких институциональных изменений в организации образовательного процесса как на уровне информационного пространства образовательных учреждений, так и на уровне взаимодействия преподавателей и учеников, которые должны быть нацелены на формирование информационной культуры личности.

Суть этих преобразований состоит не только в расширении спектра новых ИКТ, предназначенных для ознакомления обучающихся и привития навыков их использования, но и во внедрении этих технологий в жизнь учебного заведения. Особое значение в этой связи приобретают технологии, поддерживающие управление знаниями (knowledge management). К ним можно отнести:

- системы добычи данных и текстов (Data mining, Text Mining) — распознавание образов, выделение значимых закономерностей из данных, находящихся в хранилищах или входных или выходных потоках.;
- системы управления документооборотом (Document management) — хранение, архивирование, индексирование, разметка и публикация документов;
- средства для организации совместной работы (Collaboration) — сети Intranet, технологии группой работы, синхронные и асинхронные конференции;
- корпоративные порталы знаний (Enterprise Knowledge Portal)
- средства, поддерживающие принятие решений (Decision support) — экспертные системы, системы, поддерживающие дискуссионные группы и т.д.

Сегодня качественным критерием информатизации является смена целевых установок образования как социального института. В индустриальную эпоху господствовала монологическая модель трансляции знаний (учитель говорит – я слушаю), а сейчас преподаватель является не только носителем знания, но и помощником в поиске, оценке, обработке и представлении самостоятельно полученной информации

Сказанное предполагает параллельное развитие технологической и содержательной частей педагогических компонентов. Технологическая предполагает увеличение количества компьютеров, наличие постоянного доступа к быстрому Интернету, содержательная компонента – обучение педагогов, внедрение в их деятельность современного программного обеспечения управления знаниями.

Особенности ИКТ, которые необходимо учитывать в организации процесса обучения: важна не информация сама по себе, а знания, полученные в результате ее переработки, прошедшие интериоризацию, т.е. этап личностного присвоения. Для личностной и профессиональной социализации человека необходимы методы работы с информацией, позволяющие получить информационный максимум за единицу времени;

Интернет для отдельных личностей является средой обитания, они могут работать с множеством источников одновременно;

- людей не устраивает монологическая модель информационной передачи. Авторитет единственной точки зрения отменяется из-за полиморфизма информационных источников. Человек находится в среде постоянного информационного выбора;
- человек обладает информационной компетентностью, исходя из которой, человек отбирает информацию из различных источников, сумма этой информации составляет знание;
- важна не сумма знаний, а методы их приобретения.

Использование ИКТ интенсифицирует развивающийся характер образовательной деятельности. В процессе образования происходит смена ментальных моделей – меняются картины профессиональной деятельности, развиваются способности, меняются смысловые установки и ценности.

В докладе рассматриваются вопросы влияния современных ИКТ на организацию процесса обучения посредством включения в образовательный процесс наряду с преподавателями и учениками различных источников знаний и многократного повторения циклической модели обучения (Колб, Фрай) с учетом индивидуальных стилей обучения.

Копыльцов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Смольный институт Российской академии образования

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В СРЕДНЕМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАНИИ

Методы компьютерного моделирования проникают во все области человеческой деятельности, а также в такие естественные и гуманитарные науки, как физика, химия, биология, экономика, лингвистика, изобразительное искусство, музыка, психология, социология и другие. Поэтому, чем раньше учащиеся средних профессиональных училищ познакомятся с основными идеями и методами компьютерного моделирования в своей профессиональной области, тем успешнее будет их дальнейшая деятельность. Компьютерное моделирование позволяет исследовать какой-либо объект или процесс в изолированном виде, выделять нужные характеристики как бы в изолированном виде. Это позволяет без излишних ресурсов исследовать какой-либо объект либо процесс. В последние десятилетия наблюдается тенденция, что в различных областях исследования разрабатывается свой специфический для данной области математический аппарат, например, в физике, химии и др. Поэтому, сначала необходимо построить математическую модель исследуемого объекта или явления, а после этого составить алгоритм и реализовать его на компьютере. Для построения эффективных математических моделей необходимо обладать понятийным мышлением. В работах выдающегося советского психолога Льва Выготского понятийное мышление определяется через следующие три важные составляющие:

1. умение выделять суть объекта исследования или явления;
2. умение видеть причину и прогнозировать последствия;
3. умение систематизировать получаемую информацию и строить целостную картину объекта исследования или явления.

Под умением выделять суть объекта исследования или явления понимается то, что человек может выделить из потока информации ту информацию, которая является существенной для рассматриваемого объекта исследования или явления, т.е. может отделить зерна от плевел. Под умением видеть причину и прогнозировать последствия понимается, что в любом явлении человек может догадаться, что предшествовало наблюдаемому явлению и к чему может привести наблюдаемое явление. Под умением систематизировать получаемую информацию и строить целостную картину явления понимается, что человек может систематизировать информацию, которую он получает через органы чувств и мысленно построить целостную картину явления, которая не противоречит целостной картине окружающего мира.

Понятийное мышление не может ни передаваться по наследству, ни возникнуть само собой в процессе жизненного пути. Его можно развить, только изучая естественные науки, такие как, например, математика, физика, химия, биология и др.

Естественные науки отличаются от гуманитарных тем, что в них вводятся первичные понятия и на их основе строится логически обоснованное здание науки. Если обучение повторяет историческое развитие науки (исторический подход), то у учащихся на примере выдающихся ученых прошлого и результатов их исследования, вырабатывается умение выделять суть объекта исследования или явления, умение в каждом явлении видеть причины и следствия, умение систематизировать и строить целостную картину мира, т.е. в итоге формируется понятийное мышление. Обладая понятийным мышлением, учащийся сможет либо решать практически любые задачи, либо определять возможные направления, по которым возможно достичь решения поставленных задач. Более того обладая понятийным мышлением можно самостоятельно ставить новые задачи, поскольку будет ясна общая картина и тенденции ее изменения.

Для развития понятийно мышления в настоящее время большую роль может играть математическое и компьютерное моделирование. При моделировании важно выделить основные параметры, которые характеризуют суть явления или объекта исследования.

При компьютерном моделировании можно благодаря многократному прогону программы выявить, какие параметры существенны, а какие не очень. Более того, можно ранжировать параметры по степени их влияния на объект исследования или явление. С помощью компьютера так же легко видеть причины (входные параметры и их численные значения) и последствия изучаемого явления (выходные параметры и их значения).

Систематизация полученных данных при расчете на компьютере также будет способствовать развитию умения систематизировать и строить целостную картину изучаемого явления. Таким образом, математическое и компьютерное моделирование не только дает новые знания, умения и навыки в профессиональной деятельности, но и развивает понятийное мышление, которое лежит в основе интеллектуальной деятельности и которое нужно развивать на начальном и особенно на среднем этапе профессионального образования.

Костюченко О.А.
Россия, Санкт-Петербург, Детская студия мультимедиа «M-Art» Санкт-Петербургского Центра творческого развития и гуманитарного образования детей «На Васильевском» Президентская библиотека имени Б.Н. Ельцина

МУЛЬТИМЕДИЙНОЕ ПРОЕКТИРОВАНИЕ В ДЕТСКОМ ОБРАЗОВАНИИ. МУЛЬТИМЕДИЙНЫЙ ФИЛЬМ «МЫ И КОСМОС»

Проект подготовлен Детской Студией Мультимедиа «M-Art», Центра творческого развития и гуманитарного образования «На Васильевском», при поддержке Президентской библиотеки и участии Петербургского планетария.

Дети студии создали мультимедийную школьную презентацию, содержащую в себе все основные предметы школьной программы. Работа раскрывает многоаспектность проблемы космос и её связь со многими видами жизнедеятельности человека.

Мультимедийный фильм делится на части в соответствии с обязательным набором школьных уроков: русский язык, литература, история, физика, химия, биология, география, обществознание.

Все действо происходит в режиме Multi-touch – «множественное касание» функция сенсорных систем ввода (сенсорный экран, сенсорная панель). В предложенном предметном меню детская рука выбирает пункт. Далее происходит наиболее подробное освещение одной выбранной темы с использованием, анимации, кинетической типографики и спецэффектов.

Информационным поводом для создания мультимедийного фильма послужил 55-летний юбилей со дня первого полета в космос Юрия Гагарина, имеющий огромное значение не только для нашей страны, но всего мира.

В связи с этим знаменательным событием Президентская библиотека, Федерация космонавтики России и Санкт-Петербургский государственный институт кино и телевидения организовали и провели кинофорум «Кино и космос: объединяя прошлое и будущее», в программе мероприятий которого состоялся международный конкурс экранного творчества «Далекий и близкий космос».

Проектная совместная работа детей и взрослых профессионалов осуществлялась в несколько этапов:

Первый – формирование содержания проекта, методической базы и технического задания для всех групп детей участвующих в проекте.

Второй – составление и редактура текстов, которые не только в дальнейшем были озвучены детьми, но были интегрированы в видеоряд с использованием приемов мультимедийной кинетической типографики.

Третий, самый трудоемкий этап это создание детьми под руководством педагогов студии всех частей фильма. Руководствуясь заранее подготовленным индивидуально для каждого ребенка техническим заданием, все дети-участники проекта трудились, приходя на занятия в студию после школы. Создавали изображения для слайд-шоу и монтировали их. Анимировали планеты и руки для сцен с интерактивным меню multi-touch. Старшие группы интегрировали все составляющие видеоряда в свою часть работы – сцены с предметным меню и содержанием разделов.

Четвертый – озвучение. Озвучение проходило в звукозаписывающей студии Президентской библиотеки одной из лучших в городе.

Группа детей студии из 9 человек, не обладая навыками актерского мастерства и специальной подготовкой, тем не менее, замечательно справились со своей задачей. Все школьные предметы очень гармонично озвучиваются детскими голосами, сменяясь различными возрастными интонациями мальчиков и девочек.

Пятый этап проектирования – монтаж. Эту ответственную и самую сложную часть работы по детскому студийному проектированию берет на себя руководитель проекта. В задачу входит не только выстраивание всех готовых частей в единый видео ряд, но предварительное исправление всех ошибок и дополнение визуальными акцентами всех сцен фильма в контексте общего содержания.

Шестой этап – тестирование и публикация. Тестирование осуществляется сразу несколькими группами людей. Многократно фильм просматривается самими участниками проекта и сторонними зрителями еще до момента публикации в публичном интернет пространстве. Найденные ошибки, не точности исправляются, удаляются. По необходимости добавляются фрагменты, которые делают фильм еще более художественно выразительным. Затем окончательная запись и публикация проекта.

Сразу после завершения проекта мультимедийный фильм стал участником и призером международного конкурса «Кино и космос: объединяя прошлое и будущее», получив 3 место. В составе работ-призеров проект вошел на национальную электронную коллекцию Президентской библиотеки.

Лаптев В.В., Баранова Е.В., Симонова И.В.
Россия, г. Москва, Российская академия образования
Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ХАРАКТЕРИСТИКА ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ДЛЯ НЕПРЕРЫВНОЙ ПОДГОТОВКИ УЧИТЕЛЕЙ ИНФОРМАТИКИ В ПЕДАГОГИЧЕСКОМ ВУЗЕ

Для системы высшего образования с 2015 года при поддержке государства реализуется проект «Национальная платформа открытого образования», бесплатные онлайн-курсы для освоения образовательных программ бакалавриата и специалитета в вузе. В настоящий момент на платформе представлено девять общеобразовательных курсов, непосредственно ориентированных на подготовку студентов в области образования и педагогических наук, и ряд других, которые могут быть использованы при подготовке учителей, в том числе по информатике. Все эти ресурсы, в первую очередь, представляют содержание предметных областей, не моделируют деятельность учителя в реальных педагогических условиях, что затрудняет их использование при методической подготовке студентов.

Многолетний опыт преподавания информатики и информационных технологий в педагогическом вузе, в условиях трехуровневой подготовки, позволяет авторам оценить важность использования ЭОР для: обеспечения стандартизации содержания дисциплин, выстраивания индивидуальных образовательных маршрутов, предоставления возможности для самостоятельной аудиторной и внеаудиторной работы, развития дополнительной мотивации к овладению педагогической профессией.

Бакалаврам, будущим педагогам, необходимы разнообразные примеры реальной деятельности учителя на уроке, которые сложно представить в ходе аудиторных занятий, характеризующие способы представления содержания обучения, стиль преподавания, используемые методы и технологии обучения и т.д. Банк ЭОР, моделирующих различные аспекты деятельности учителя, позволит студентам в сжатые сроки познакомиться с вариантами деятельности учителя в различных условиях и ситуациях, выбрать для себя наиболее подходящие и интересные. Преподаватель блока методических дисциплин может формировать из материалов ЭОР различные задания для самостоятельной работы студентов, например, создать тест по одной из тем школьного курса информатики, разработать конспект урока на основе материалов ЭОР или задания для учащихся с использованием какого-либо средства информационных технологий. Наличие такого банка позволит существенно усилить практическую составляющую и интерес студентов к методической подготовке.

Методическая подготовка будущего учителя информатики в магистратуре ориентирована на старшую школу в условиях базового и профильного уровня. Для магистратуры банк ЭОР предложенной структуры и состава необходимо расширить, дополнить объектами с новым учебным содержанием и заданиями по работе с объектами, в том числе, и сложными, предполагающими самостоятельное создание объектов для ЭОР.

Сложно переоценить значимость внешнего оценивания исследований аспирантов на базе открытого широкого обсуждения всем научно-педагогическим сообществом, которое будет способствовать объективному выявлению как наиболее интересных, значимых, инновационных, так и слабых, несостоятельных исследований. Механизм реализации такого обсуждения может осуществляться с использованием специализированного сайта, который обеспечит возможность коммуникаций внутри научно-педагогического сообщества по направлениям подготовки.

Специальные классы электронных образовательных ресурсов должны быть представлен в вузе для организационного сопровождения процесса обучения, предоставления публичного доступа к документации по образовательным программам в сети Интернет и электронные портфолио обучающихся - среда для создания и хранения структурированной информации о достижениях обучающихся в процессе освоения образовательных программ всех уровней.

Разработка ЭОР для трехуровневой подготовки в педагогических вузах учителей информатики, специалистов в области информатизации образования должны отвечать как общим требованиям к онлайн-курсам открытого образования, так и специфическим для педагогического образования, обеспечивать методическую функцию, функцию сопровождения индивидуального маршрута студента и представления в открытом доступе результатов освоения образовательной программы.

Марченко Е.П.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена

МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ПОДГОТОВКЕ ПЕДАГОГА-МУЗЫКАНТА К ДУХОВНО-НРАВСТВЕННОМУ ВОСПИТАНИЮ МОЛОДЕЖИ В ШКОЛЕ ЦИФРОВОГО ВЕКА

Осуществление процесса духовной коммуникации в художественном пространстве музыкального искусства и образования становится реальным воплощением гуманистической образовательной парадигмы, одухотворенной и пронизанной чувством любви и согласия. Процесс духовной коммуникации, рождение эстетической эмпатии, открывающей необозримое пространство

для творчески-созидательной деятельности, формирует у будущего профессионального музыканта чувство сопринадлежности к некоему коллективному целому. А «сознание, выражаемое в слове «мы», есть естественная основа всякого индивидуального самосознания, всякого «я».

Музыкальное искусство играет особую, ничем не заменимую роль в воспитании, и эта особенность вытекает прежде всего из того обстоятельства, что любое произведение искусства в самом себе содержит нравственное начало. В музыке нравственное содержание – воспевание добра и осуждение зла – является, можно сказать, смыслом его существования, основной силой его воздействия.

Формирование ценностно-смысловой сферы личности продолжается на протяжении всей жизни. Ее содержание может меняться под влиянием многих факторов, так как социализация может происходить как в условиях стихийного воздействия на личность различных обстоятельств жизни в обществе, имеющих иногда характер разнонаправленных факторов, так и в условиях воспитания, т.е. целенаправленного формирования личности.

Знание современных инновационных подходов к организации общего музыкального образования может быть полезным как в плане разработки необходимых музыкально-образовательных технологий, так и в отношении создания нового поколения стандартов высшего и специального музыкально-педагогического образования.

Музыка есть продукт группового поведения и поэтому, несомненно, зиждется на определенных законах, созданных обществом. Но при этом она обладает способностью создавать новую общность, объединять людей в едином духовном порыве, формировать новое пространство культуры, новую уникальную художественную реальность. Это является важнейшей функцией музыки как вида искусства.

Одним из наиболее дискуссионных вопросов на сегодняшний день является проблема внедрения информационных технологий (ИТ) – мощнейшего образовательного и воспитательного ресурса в Школе цифрового. Обучение музыке, в особенности исполнительских и творческих направлений, требует непосредственного «живого» общения обучаемого с педагогом. Творчество как компонент формирования личности учителя должно присутствовать на всех этапах ее становления, стать ведущим системообразующим компонентом учебно-воспитательного процесса.

Одно из основных направлений применения ИТ в образовательном процессе связано с развитием музыкально-компьютерных технологий (МКТ) и электронного музыкального инструментария (ЭМИ) в Школе цифрового века.

Важная задача современного этапа развития музыкальной педагогики и педагогических исследований в данном направлении заключается в том, чтобы раскрыть дидактические особенности использования МКТ, возможности их применения в музыкальном воспитании и образовании на основе классической музыки, традиционных подходов к способам трансляции многовековой музыкальной культуры. Важно, чтобы увлечение внешними, новыми, цифровыми эффектами и возможностями способствовало не только получению ярких и красочных впечатлений в общении с музыкальным искусством, но и развивало критическое мышление, способствовало интеллектуальному и культурному росту учащихся.

Митрофанова А.В., Ковальногова Н.М., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

МЕТОДЫ АВТОМАТИЗИРОВАННОГО ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ПОСТРОЕНИЯ ИНДИВИДУАЛЬНОЙ ТРАЕКТОРИИ ОБУЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Наряду с понятием индивидуальная образовательная траектория существует понятие индивидуальный образовательный маршрут (далее – ИОМ). Часто эти понятия употребляются как синонимы, но это не совсем правильно. ИОМ – это проект индивидуально-дифференцированного освоения основной образовательной программы, обеспечивающий студенту вуза как субъекту учебно-профессиональной деятельности позицию субъекта выбора индивидуальной образовательной траектории. Следовательно, участники образовательных отношений со стороны образовательной организации в целях обеспечения ИОТ формируют ИОМ, руководствуясь которым обучающиеся и их родители в праве сформировать ИОТ.

Много работ посвящено обоснованию необходимости использования ИОТ и основным аспектам ее использования (необходимости создания специальных организационно-педагогических и психолого-педагогических условий и пр.), однако на данный момент совсем немного информации о практике построение ИОТ (особенно об автоматизации этого процесса).

Одним из наиболее ярких примеров является адаптивная образовательная платформа от компании Knewton, которую можно подключить к любой современной системе управления учебным процессом (LMS). Методология Knewton строится вокруг двух основных понятий: технологии планирования образовательной траектории и сложной модели оценки студента. Такой подход в корне отличается от большинства “адаптивных приложений”, которые по сути применяют адаптивный подход к единственной точке, в которой измеряются знания студентов. Примером такого

“слабоадаптивного” подхода является диагностический экзамен, по результатам которого компьютер определяет какой контент будет показан студенту в дальнейшем. Технологии data mining и персонализации используются здесь минимально или не используются вообще.

Адаптивное обучение в понимании Knewton должно реагировать в реальном времени на результаты отдельного студента и его действия в системе. Этот подход увеличивает вероятность того, что студент получит правильный образовательный контент в нужный момент и достигнет поставленных перед собой целей. К примеру, если студент плохо справляется с определенным набором вопросов, то Knewton сможет предположить, какие темы, затронутые в этом списке вопросов, оказались непонятными и предложить ему контент, который поможет повысить уровень понимания именно этих тем.

Данные которые использует адаптивная платформа собираются самим образовательным приложением и передаются на сервер Knewton с использованием API. Чтобы начать собирать определенный вид данных, например, когда студент начал смотреть видео или результат ответа на вопрос, достаточно добавить одну строчку кода, которая будет передавать эти данные Knewton. Адаптивная платформа анализирует собранные данные и возвращает их приложению в виде рекомендаций преподавателю или указания, какой блок контента нужно показать студенту следующим.

Несмотря на огромные и очевидные успехи в апробации данной платформы и применения адаптивного обучения в целом, есть немало критики данного подхода. В первую очередь специалисты отмечают не универсальность подхода Knewton (Knewton исходит из того, что всегда есть правильный ответ). Другой вопрос, который часто возникает в связи с Knewton — это использование персональных данных. Knewton утверждает, что не хранит персональных данных студентов. По словам Джозе Феррейра (основателя Knewton): “Мы помогаем студенту понять его образовательную историю, не сохраняя его идентификационную информацию”.

Развитие средств телекоммуникаций позволяет экспертам прогнозировать появление полноценных возможностей приобретения нужных знаний, навыков и компетенций по индивидуальным траекториям обучения в любом возрасте и в любой точке пространства. Подобная концепция потребует от вузов такого планирования и организации учебного процесса, когда на первом месте будут стоять не планы, а желания студентов и возможности преподавателей. Такой подход имитирует законы рынка – как преподаватели предлагают набор курсов, а студенты изъявляют желание их изучать, так и студенты выставляют запросы на формирование дисциплин с определенными компетенциями и содержательной частью, а преподаватели данные курсы разрабатывают.

Использование ИОТ способствует вовлеченности обучающихся в образовательный процесс. Право выбора позволяет реализовываться абитуриенту как личности, тем самым развивая свои способности и удовлетворяя своим интересам.

Митрофанова А.В., Ковальногова Н.М., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРЕДПОСЫЛКИ СОЗДАНИЯ АВТОМАТИЗИРВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ОБУЧАЮЩЕГОСЯ ПРИ ПОСТРОЕНИИ ИНДИВИДУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ТРАЕКТОРИИ В РАМКАХ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ

В настоящее время образование развивается достаточно динамично. Эффективное развитие образования направлено на обеспечение доступности качественного образования, отвечающего требованиям современного инновационного развития страны. В связи с этим появляются новые формы и способы обучения, открывающие новые возможности как для преподавателя, так и для обучающегося. Согласно Постановлению Правительства РФ от 23 мая 2015 г. №497 «О Федеральной целевой программе развития образования на 2016 - 2020 годы» в рамках задачи 5 «Формирование востребованной системы оценки качества образования и образовательных результатов» предусмотрена реализация следующих мероприятий: «будут разработаны механизмы и типовые модели хронологической оценки учебных достижений обучающихся, позволяющие формировать траектории индивидуального развития обучающихся в средних профессиональных образовательных организациях и образовательных организациях высшего образования». Это говорит о том, что обучение приобретает личностный характер, у обучающихся появляется возможность самореализации и построения индивидуальной образовательной траектории, а также методов автоматизированной поддержки обучающегося при ее выборе.

Если рассматривать Приказ Министерства образования и науки РФ от 12 ноября 2015 г. №1327 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.01 Экономика (уровень бакалавриата)» (далее ФГОС №1327), то пункт VI «Требования к структуре программы бакалавриата» утверждает, что структура программы бакалавриата включает обязательную часть (базовую) и часть, формируемую

участниками образовательных отношений (вариативную). Это обеспечивает возможность реализации программ бакалавриата, имеющих различную направленность (профиль) образования в рамках одного направления подготовки (далее - направленность (профиль) программы).

Согласно подпункту 6.3 ФГОС №1327 при разработке программы бакалавриата обучающимся обеспечивается возможность освоения дисциплин (модулей) по выбору, в том числе специальные условия инвалидам и лицам с ограниченными возможностями здоровья, в объеме не менее 30 процентов объема вариативной части Блока 1 "Дисциплины (модули)", который включает дисциплины (модули), относящиеся к базовой части программы и дисциплины (модули), относящиеся к ее вариативной части. Вариативная часть Блока 1 составляет 107-116 зачетных единиц (далее з.е.) следовательно, дисциплины (модули) по выбору обучающимся могут быть в объеме 32-34 з.е.

Таким образом, имеет место быть индивидуальная образовательная траектория (вариативное обучение). С одной стороны использование вариативного обучение дает обучающемуся свободу выбора, но с другой стороны не каждый сможет этой свободой правильно воспользоваться. В связи с этим наряду с вариативным обучением должна существовать автоматизированная система поддержки обучающегося при выборе индивидуальной образовательной траекторией.

Морозов С.А.
Россия, г. Курск, Курский музыкальный колледж-интернат слепых

РОЛЬ СОВРЕМЕННЫХ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ СТУДЕНТОВ – ИНВАЛИДОВ ПО ЗРЕНИЮ В СРЕДНИХ ПРОФЕССИОНАЛЬНЫХ МУЗЫКАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЯХ.

Развитие средств вычислительной техники, а особенно появление компьютерных программ экранного доступа (screen reader), привело к созданию новых форм в учебном процессе при обучении людей с ограниченными возможностями по зрению, переосмыслению методики преподавания как традиционных дисциплин, так и новых предметов, связанных с музыкальными компьютерными технологиями.

Использование компьютерных технологий в обучении инвалидов по зрению из многообещающих инновационных проектов уже превратилось в реальность.

Самый главный дефицит для незрячего человека – дефицит информации восполняется с помощью цифровых технологий, в частности, компьютеров, смартфонов и т.д. благодаря программам речевого сопровождения.

Расширяются возможности включения незрячих в инклюзивное музыкальное образование. Там, где раньше можно было проверять знания и умения только в устной форме (прежде всего это теоретические дисциплины: теория музыки, гармония, полифония, сольфеджио), появилась возможность работать с программами нотно-компьютерной графики.

Совместный проект Sibelius и NVDA обеспечивает экранный доступ с речевым сопровождением для работы со сложными нотными текстами. Профессиональные возможности программы постепенно адаптируются для полноценного озвучивания того, что мы видим на экране. Это, прежде всего, ввод, редактирование и прочтение визуального нотно-графического материала – то, что в первую очередь не хватало как студентам, так и преподавателям теоретических дисциплин.

Незрячие композиторы получили возможность самостоятельно набирать нотный текст и подготавливать его для дальнейшего опубликования. Это многократно ускорило претворение в жизнь творческих идей авторов, так как нотные тексты раньше приходилось сначала писать рельефно-точечным способом по системе Брайля, и только потом надиктовывать материал или отдавать специально обученному переписчику брайльских нот. А таких специалистов очень мало не только в нашей стране, но и в мире.

Появляется реальная возможность реализации обучения инвалидов по зрению новым, ранее недоступным направлениям в профессиональной деятельности.

Курский музыкальный колледж-интернат слепых является практически единственным специализированным музыкальным учебным заведением в мире. Вся многолетняя деятельность колледжа направлена не только на воспитание полноценного специалиста в выбранной профессии, но также и на его интеграцию в современное общество.

Овладение музыкально-компьютерными технологиями в совокупности с творческим потенциалом дает не только стимул к дальнейшему профессиональному росту, но и предполагает приобретение дополнительной, востребованной на сегодняшний день, специальности аранжировщика.

Одним из удачно адаптированных виртуальных секвенсоров для незрячих музыкантов является программа Sonar от компании Cakewalk. При поддержке Jaws практически весь функционал программы доступен для использования незрячим человеком

То, что компьютерные технологии необходимы в обучении студентов музыкальных специальностей ни у кого не вызывает сомнений, хотя в большинстве случаев ситуация такова, что полноценно воплотить в учебный процесс эти предметы удаётся далеко не каждому учебному

заведению. Основные причины тому нехватка квалифицированных специалистов и материально-технические проблемы. Курский музыкальный колледж-интернат слепых на сегодняшний день в полном объеме реализует данные дисциплины, имея в своем арсенале самые современные технические средства, профессионально подготовленные педагогические кадры, специально оборудованные аудитории с возможностью самостоятельных занятий студентов.

И в заключение попытаемся перечислить некоторые дополнительные направления деятельности будущих выпускников – инвалидов по зрению, владеющих современными музыкально-компьютерными технологиями:

- создание аранжировок, инструментовок и оригинальных композиций;
- запись «живого» звука;
- профессиональный набор нотного текста;
- реставрация старых записей;
- подготовка цифровых фонограмм;
- синтез звука;
- звукорежиссерская работа.

Николаева Д.С.
Россия, Санкт-Петербург, Школа № 53 Приморского района Санкт-Петербурга,
Российский государственный педагогический университет им.А.И.Герцена

МЕЖДУНАРОДНЫЕ УЧЕБНЫЕ ПРОЕКТЫ В РАМКАХ КУРСА ИНФОРМАТИКИ И ИКТ В КОНТЕКСТЕ ИНКЛЮЗИВНОГО ОБРАЗОВАНИЯ

С 1 сентября 2016 года вступил в силу ФГОС инклюзивного образования, предполагающий, что любая школа должна быть готова к обучению детей с ОВЗ вместе с обычными ученикам.

Если принять во внимание, что главная задача инклюзии – социализация, становится очевидным тот факт, что одним из наиболее результативных для особенных детей может стать метод проектов. Эта гипотеза подкрепляется немалым объёмом успешного педагогического опыта в области применения метода проектов в инклюзивном образовании, накопленным на сегодняшний момент.

Говоря о современной ситуации в области применения метода проектов, нельзя не отметить, что одной из обязательных составляющих любой подобной работы становится применение информационно-коммуникационных технологий. По этой причине возрастает роль информатики как предмета, на базе которого может быть составлена программа с применением метода проектов как одного из основных подходов к обучению в школах с инклюзивным компонентом.

Особое место среди учебных проектов занимает международный проект.

Учитывая тенденции приведения российской системы образования в соответствие с международными стандартами, роль международных учебных проектов оценивается достаточно высоко как для учащихся, так и для учителя.

Международные проекты на уроках информатики позволяют, прежде всего, обогатить содержание курса.

Собственный опыт работы в школе с инклюзивным компонентом, основанный на выполнении международных проектов, показал высокую результативность подобного подхода. Можно с уверенностью сказать, что выполнена задача адаптации инклюзивных детей к современному миру, их социализации, получены навыки самостоятельного проведения исследований и выполнения практических задач.

В ходе обобщения этого опыта были выделены основные этапы работы над международным учебным проектом, примерные сроки их выполнения и роль учителя на каждом из этапов; разработаны примеры заданий для учебных проектов разной направленности и разного уровня сложности. Актуальной задачей на сегодня представляется систематизировать накопленные наработки в виде завершённой рабочей программы по информатике для школ с инклюзивным компонентом, включающей в себя интегрированные предметные области «Математика», «Естествознание», «Технология», «Филология».

Носкова Т.Н., Павлова Т.Б., Тумалева Е.А. Яковлева О.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

СОЦИАЛЬНЫЕ МЕДИА КАК ФАКТОР ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ СПЕЦИАЛИСТА В ОБЛАСТИ ОБРАЗОВАНИЯ

Сегодня для конкурентоспособности в профессиональной сфере недостаточно овладения только знаниями и компетенциями в соответствии со стандартом. Среда электронного взаимодействия ставит перед специалистами новые цели, требует обеспечения возможности реализации передовых образовательных стратегий на пороге шестого технологического уклада (уровня развития производительных сил), который, как считают специалисты по прогнозам, начинает

оформляться в 2010—2020 годах, а в фазу зрелости вступит в 2040-е годы. При этом в 2020—2025 годах произойдёт новая научно-техническая и технологическая революция, основой которой станут разработки, синтезирующие достижения наукоёмких, или, как часто определяют, «высоких технологий». Очевидно, что в опоре на компьютерные средства и технологии уже сегодня необходимо реализовывать принцип новых задач образовательной практики, а именно выход за рамки стандарта, опережение, научный и технологический прорыв.

Социальные медиа приобрели популярность у молодежи как инструмент поддержания социальных связей. Они широко используются для решения образовательных задач как основа новых коммуникационных форматов. Специалисты в области образования должны знать возможности, ограничения и риски социальных медиа с целью использования их уникальных возможностей для совместного обучения, творчества и профессионализации. В качестве ответа на вызов активно развивающейся электронной среды кафедра методики информационного и технологического образования института компьютерных наук и технологического образования РГПУ им. А.И. Герцена уже третий год реализует совместно с Институтом ЮНЕСКО по информационным технологиям образовательный модуль «Социальные медиа и современные образовательные практики» с выдачей международного сертификата. Цель модуля – формирование компетенций современных специалистов в области образования в использовании медиа среды для решения образовательных задач. Эти новые компетенции дают возможность повысить конкурентоспособность выпускников магистратуры. Изначально модуль осваивали магистранты кафедры (магистерская программа – «Информационные технологии в образовании»), ориентированные в соответствии с профилем программы на тематику модуля. В 2016 году к изучению курса подключились магистранты других институтов и факультетов РГПУ им.А.И.Герцена. Это ответственный и важный опыт апробации, как содержания программы модуля, так и возможной формы организации деятельности студентов и преподавателей.

Современный педагог должен иметь компетенции, позволяющие подготовить детей и подростков к взаимодействию с широкой средой социальных медиа. Именно поэтому в содержание модуля входят такие вопросы, как новые социально-психологические явления в среде глобальных взаимодействий; социальные медиа: понятие, социальная значимость, педагогический потенциал; задачи медиа образования; роль социальных медиа в образовательной среде; вопросы проектирования медиа-среды для решения конкретных образовательных задач; Интернет-сервисы социальных медиа и методики виртуальных образовательных взаимодействий на основе социальных медиа. Курс реализован в очно-дистанционной форме с использованием системы управления обучением Moodle. Магистранты осваивают теоретические материалы курса, выполняют практические задания, а также описывают концептуальную идею своего проекта за полтора месяца. Большое значение имеет методика подачи материала (проблемные вопросы, практические примеры, презентации с аудио комментариями преподавателя и др.) и методика организации взаимодействия магистрантов и преподавателей. Все проблемные вопросы обсуждаются на форуме курса, многие задания предполагают взаимное комментирование. Преподаватели выступают преимущественно в роли тьюторов, направляя активность участников.

Многие проекты, разработанные обучаемыми, имели социальную направленность. Они могут быть разделены на две группы - ориентированные на изменение корпоративной университетской среды (поддержка студенческих инициатив, социальных проектов под эгидой университета), а также направленные на изменение общей социально-культурной среды (развитие профессиональной деятельности социального педагога; инклюзивное, неформальное и информальное образование; создание сообществ обмена положительным опытом).В процессе изучения модуля каждый магистрант проектировал часть электронной образовательной среды, через которую, используя средства социальных медиа, он готовился к решению будущих профессиональных задач. В образовательной практике уже стали популярными такие модели, реализуемые на основе социальных медиа, которые разворачиваются параллельно в аудиторной и электронной образовательной среде. Однако в результате освоения модуля магистранты смогли выйти на более высокий уровень - проектировать такие образовательные практики, которые запускаются в сетевой среде взаимодействий и разворачиваются в электронных форматах. Можно с уверенностью утверждать, что эти практики являются инновационными.

Нымм В.Р., Пиотровская К.Р., Еремеева Ю.П., И.С. Макогон
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

СТАТИСТИЧЕСКИЕ МЕТОДЫ В КОМПЬЮТЕРНОЙ ЛИНГВОДИДАКТИКЕ

В течение ряда лет междисциплинарная исследовательская группа РГПУ им. А.И. Герцена развивает исследования по проблеме компьютерного обучения иностранным языкам. Основные положения развиваемой группой концепции отражены в статьях и монографиях последнего десятилетия.

В качестве основного инструмента исследований используется программа компьютерного обучения и тестирования, разработанная в 2005 году на филологическом факультете университета. Она объединяет в одной оболочке функциональные модули, реализующие практически все основные типы упражнений типа “стимул - реакция”, на основе которых строятся современные учебники иностранного языка. Программа предназначена для использования студентами как при выполнении заданий учебного плана по изучению иностранного языка, так и при выполнении ими (в рамках курсовых и выпускных квалификационных работ) научных и научно-педагогических исследований по проблеме компьютерного языкового обучения.

Реализуемые программой алгоритмы управления процессом обучения основаны на методах стохастической теории обучения. Р. Буша и Ф. Мостеллера.

Программа снабжена средствами сбора данных о реакциях обучаемого в ходе обучения с целью: а) последующей обработки полученной информации и формирования новых знаний о процессах компьютерного обучения иностранным языкам; б) использования этих знаний для постановки новых задач исследования, создания новых и корректировки существующих алгоритмов управления процессами обучения. Тем самым реализуется механизм параллельного развития как самой программы, так и проводимых с ее помощью исследований.

В настоящее время ведутся совместные работы филологического факультета, лаборатории инженерной лингвистики и института компьютерных наук и технологического образования РГПУ им. А.И. Герцена по созданию сетевой версии программы на базе языка Python.

Другой важной составляющей эффективности (наряду с организацией процесса обучения и управлением им) является отбор содержания обучения. Оптимизация процесса формирования иноязычной профессиональной компетенции сопряжена, с одной стороны, со все ускоряющимися темпами информационного обмена, который ведет к изменчивости лексико-грамматического состава профессионально ориентированного языка, с другой, - с появлением новых открытых сервисов, позволяющих оперативно осуществлять автоматизированные статистические отбор и исследование учебных текстов, для формирования базы языковых упражнений в области лексики и грамматики.

Хотя объективные методы отбора учебных терминологических единиц (например, статистико-вероятностный подход, получивший свое развитие в работах научных школ Р.Г. Пиотровского и Р. Кёллера) известны с шестидесятых годов XX века, до сих пор отбор терминологических единиц для изучения в рамках профессионально ориентированного языка производится подчас субъективно, исключительно с опорой на личный опыт, компетентность и интуицию преподавателя или исследователя.

Сегодня статистико-вероятностный подход переживает определенный ренессанс. Он вновь востребован, на что указывают работы группы исследователей из Японии и Новой Зеландии. Эта группа создала ряд открытых сервисов, под названием AntConc, которые могут быть использованы в корпусных исследованиях и, в частности, при отборе содержания обучения.

В настоящее время на базе открытых веб-сервисов группы AntConc нами разрабатывается технологическая цепочка операций по квантитативному отбору содержания обучения и созданию информационного обеспечения программы. Организованный таким образом комплекс будет служить поддержкой преподавания таких дисциплин как «Квантитативная лингвистика и новые информационные технологии», «Компьютерная лингводидактика», «Новые информационные технологии в филологии», «Сетевой инструментарий лингвиста».

Обухова Е.Н.
Россия, г. Ростов-на-Дону, Донской государственный технический университет

АНАЛИЗ РАНЖИРОВАННОЙ ОЦЕНКИ ЗНАНИЙ ПО РЕЗУЛЬТАТАМ ФАКТОННОГО ТЕСТИРОВАНИЯ

С целью упрощения и формализации задачи в целом для любого учебного материала (дидактической единицы), подлежащего тестированию, целесообразно выделить элементы знания, дальнейшее деление которых на менее содержательные компоненты невозможно или не обязательно. Назовем их факторами знаний. В этом случае на вопросы, связанные с факторами знаний, может быть дан лишь двоичный ответ. Задание теста, в зависимости от назначенной ему сложности, может включать некоторое количество факторов знаний. Не смотря на то, что факторы знаний оцениваются в двоичной шкале, в целом, благодаря соединению оценок факторов знаний, можно получить единую оценку доли полного знания, т.е. весовые оценочные коэффициенты для расшифровки уровня выполнения тестового задания и всего теста. Ключевым в таком подходе является то, что тестовое задание можно построить как совокупность микрозаданий, имеющих двоичные (двухуровневые) ответы «да» и «нет» (1 и 0).

В связи с этим предлагается процесс построения тестового вопроса рассмотреть как исследование многофакторной зависимости. Тогда к изучению и построению этой зависимости можно подойти с использованием методологии планирования многофакторных экспериментов.

Поскольку тестирование микрознаний-факторов имеет двоичную оценку, к этому процессу можно применить теорию двухуровневых многофакторных экспериментов. В этом случае множество ответов можно представить, как совокупность опытов над вопросом, результаты которых принимают значения, соответствующие его истинным свойствам как объекта исследования. Для каждого ответа-фактора существует два уровня, на которых он может варьироваться в таком условном эксперименте. Верхним уровнем является правильный (+1), а нижним уровнем – неправильный (-1). Производя варьирование факторов на двух уровнях, можно получить эксперимент, реализующий все возможные сочетания факторов – полный факторный эксперимент. Тогда, если число микрознаний-факторов выбрано при построении теста, можно найти число ответов-опытов, необходимое для реализации всех возможных сочетаний факторов. Это число и есть максимальное количество различных (правильных, неправильных, частично правильных) ответов, могущих возникнуть в тестовом задании.

Для структурирования учебного материала необходимо выделение в изучаемой теме T элементов ее знания K, названных авторами микрознаниями (МЗ). Множеству МЗ по знанию K темы T соответствует множество вопросов Q о сути этих знаний. Далее, множеству вопросов Q сопоставляется множество ответов A, которому сопоставляется множество оценок знания E.

Ответы на вопросы, поставленные относительно МЗ должны характеризоваться рядом свойств. Во-первых, они должны быть настолько элементарны, что допускать демонстрацию освоения одним правильным ответом, а незнания – одним неправильным. Во-вторых, их совокупность должна при всех правильных ответах гарантировать полное знание изучаемой темы. В-третьих, МЗ должны быть максимально независимы, т.е. владение одним из них не гарантирует однозначно владение другим, и, наоборот, незнание какого-либо МЗ не исключает знания другого. В-четвертых, условный «вес» каждого МЗ в общем знании материала темы должен быть примерно одинаков (сопоставим). Тогда степень усвоения изучаемой области учебного материала может характеризоваться долей правильных ответов по МЗ от их полной совокупности.

Каждому МЗ сопоставляется правильный и неправильный ответы. Варьирование комбинаций ответов на МЗ позволяет получить совокупность комбинированных ответов на вопрос теста, содержащую все их возможные сочетания. В этом свойстве просматривается аналогия со структурой полного факторного эксперимента. Это позволяет строить многофакторные вопросы, а варианты ответов на них формировать по методологии планирования факторных экспериментов, полностью формализуя процедуру составления тестов, делая ее объективной и независящей от предметной области оцениваемых знаний.

Предусмотренная в факторных системах вариативность не только вопросов по факторам знания, но и выбора нескольких ответов при не полностью уверенном знании, позволяет использовать дифференцированную оценку знания с оценкой среднего уровня знания и степени неуверенности этого знания. Все это расширяет возможности и результативность применения тестового подхода при реализации всех видов контроля знаний, в особенности, текущего и промежуточного контроля.

Одинокая М.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет имени Петра Великого

КОНЦЕПЦИЯ РАЗРАБОТКИ ИНТЕРАКТИВНЫХ ЭЛЕКТРОННЫХ УЧЕБНИКОВ ВУЗа

Характерной особенностью усовершенствования учебного процесса в ВУЗах является разработка электронных учебных пособий и электронных учебников. Под электронным учебником (ЭУ) понимают обучающую программную систему комплексного назначения, обеспечивающую непрерывность и полноту дидактического цикла обучения: предоставляющую теоретический материал, обеспечивающую тренировочную учебную деятельность и контроль уровня знаний, информационно-поисковую деятельность и наличие интерактивной обратной связи [2], а также методические инструкции по выполнению практических, самостоятельных работ для организации работы с ЭУ на базе информационно-коммуникативных технологий.

Из определения ЭУ следует, что он должен иметь ряд принципиальных отличий от учебника, изготовленного в типографии, а именно: возможность ознакомления с аннотацией учебного курса, учебным планом и программой дисциплины; обеспечение учебной информацией в форме лекций, наглядно-иллюстрированного материала (презентаций, аудиоматериалов, видеофрагментов, справочных материалов, гиперссылки); контрольно-измерительные материалы (эссе, электронные учебные задания для самопроверки, контроля знаний, тесты для промежуточной и итоговой аттестации).

Для создания ЭУ предлагается выполнить: разработку УМК по учебной дисциплине; создание площадки на платформе LMS MOODLE для разработки ЭУ; отбор и структурирование учебного материала ЭУ по учебной дисциплине на основе УМК в виде учебных модулей и размещение их на площадке; реализацию гипертекста в электронной форме с помощью специального программного обеспечения. Наличие в ЭУ средств гипертекста и мультимедиа позволяет представить учебный

материал в интерактивной форме, обеспечить быстрое нахождение информации; тестирование и редактирование ЭУ. При разработке ЭУ целесообразно подбирать в качестве источников печатные издания, наиболее полно соответствующие стандартной программе, удобные для создания гипертекстов и содержащие большое количество примеров и учебных заданий.

Следуя вышеизложенным этапам, преподаватели ВУЗа могут самостоятельно подготовить учебный материал и реализовать его в виде ЭУ. Дальнейшее повышение интерактивности будет более выраженным и переведено с теоретического на практический уровень при пристальном отслеживании всех этапов учебной работы педагогом [1]. Реализация указанных этапов разработки ЭУ преподавателями ВУЗов на платформе LMS MOODLE позволяет существенно повысить эффективность процесса его составления по различным, как гуманитарным, так и техническим дисциплинам.

Рассмотрены основные требования к структуре и содержанию интерактивных электронных учебников, обеспечивающие их функциональность и эффективность самостоятельной работы студентов. Уточнено понятие электронного учебника, приведены его основные возможности.

Панкова А.А.
Россия, г. Воронеж, Детская школа искусств №7 городского округа г. Воронеж

РОЛЬ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В СТАНОВЛЕНИИ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ БУДУЩИХ УЧИТЕЛЕЙ МУЗЫКИ

Эффективность применения широких возможностей информационных технологий (ИТ) в образовательном процессе сегодня не вызывает сомнения и доказана многими современными исследователями (Г.А. Бордовский, И.Б. Горбунова, М.С. Заливадный, О.А. Козлов, В.В. Лаптев, М.П. Лапчик, В.Л. Латышев, Н.В.Макарова, Л.П. Мартиросян, С.В. Панюкова, Е.С. Полат, И.В. Роберт, Б.Я. Советов, В.П. Соломин, Н.В. Софронова, О.А. Тарабрин и др.). Информатизация также затронула сферы музыкального искусства и музыкально-педагогического образования. Как отмечает ряд исследователей (Г.Г. Белов, И.Б. Горбунова, А. Камерис, И.М. Красильников, Е.А. Ложакова, Э.М. Кибиткина и др.), особой образовательной средой реализации междисциплинарного подхода, возникшей на границе двух различных областей знания — информатики и музыки, — являются музыкально-компьютерные технологии (МКТ), позволяющие открыть новые возможности для творческого эксперимента, расширить познавательный кругозор обучаемого, использовать богатый педагогический инструментарий традиционного обучения музыке и широкие возможности музыкального компьютера, оптимизировать учебный процесс, сделать его высокохудожественным и высокотехнологичным, соответствующим требованиям современной образовательной среды.

Исследование МКТ в рамках предметной области информатики и ИТ проведено рядом авторов (И.А. Большакова, И.Б.Горбунова, А.В. Горельченко, М.С. Заливадный, Э.В. Кибиткина, Е.А. Ложакова, Ж.Ю. Ситникова и др.). Э.В. Кибиткиной обоснована взаимосвязь МКТ и информатики: «МКТ можно рассматривать как часть информатики, рассматривающую алгоритмы над звуковыми или иными музыкальными данными и изучающую процессы их синтеза, передачи и обработки <...> При этом МКТ затрагивают все три основных аспекта информатики: технический (hardware) <…>; программный (software) <…>; алгоритмический (brainware)».

Построение учебного процесса с применением МКТ позволяет изучить эти основные аспекты и оценить преимущества современных ИТ, а также освоить методику их использования в музыкально-педагогической деятельности. Использование МКТ обеспечивает естественность процесса обучения ИТ будущими учителями музыки, создает новые позитивные факторы, например, в значительной степени позволяет увеличить долю и эффективность самостоятельной работы студентов, что является важным аспектом для формирования их ИК.

Исследования МКТ в рамках музыкального и музыкально-педагогического образования были проведены рядом авторов (Н.В. Белоусова, Г.Г.Белов, В.О. Белунцов, И. Б. Горбунова, С.В. Чибирев, М.С, Заливадный, А. Камерис, И.М. Красильников, С.П. Полозов и др.). Обучение ИТ будущих учителей музыки построенное базе МКТ с использованием специализированных музыкальных программно-аппаратных средств формирует знания не только в области современных ИТ, но и способствует повышению эффективности специальной подготовки педагога-музыканта, поскольку оптимизируют его образовательную и самообразовательную деятельность, углубляют ее теоретико-методическое содержание.

В процессе творческой деятельности современный музыкант должен владеть и гармонично сочетать методы работы с «живым» звуком и МКТ. Так, например, композиторы (Г.Г. Белов, Э. Денисов, М.С. Заливадный и др.) подчеркивают актуальность владения навыками работы в электронной студии для современного музыканта. Сегодня у музыканта имеется богатый спектр необходимых программных и аппаратных средств МКТ, позволяющих совершенствовать профессиональную деятельность и расширить творческие возможности за счет применения современных ИТ.

Учитывая «плодородность» информационной образовательной среды, которую образуют МКТ, а также их высокую интегрирующую способность в отношении дисциплин предметной области ИТ и музыки, использование МКТ в процессе формирования информационной компетентности (ИК) будущего учителя музыки является необходимым в условиях функционирования высокотехнологичной информационной образовательной среды.

Пелевин М.С., Богданов Т.Р.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ИТ НАПРАВЛЕНИЙ

В профессиональной деятельности, на которую ориентированы программы подготовки специалистов ИТ направлений необходимо во всех видах учебных занятий вносить элементы персонального участия и интереса участников к производственному процессу. Выпускник, освоивший программу обучения, должен обладать профессиональными компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа: проектно-конструкторская, проектно-технологическая, производственно-технологическая, организационно-управленческая, научно-исследовательская. Все программы подразумевают формирование умения проводить разработку и исследование экспериментальных моделей объектов профессиональной деятельности в различных областях производства. Направления ИТ-систем и ИТ-технологий объединяют прикладные области общей ИТ-грамотностью и компетентностью в той степени универсальности, которая должна быть натренирована у выпускников ИТ направлений обучения. В ходе учебного процесса: лекций, лабораторных и практических занятий, разделы активных форм обучения включаются с материалом, родственным заданиям учебных практик. Поддержание сквозной активной концепции профессиональной подготовки имеет практическую ценность как для прикладной, так и для академической подготовки специалистов.

Пример практического занятия, сочетающего в себе теоретическую, прикладную и практическую составляющую в концепции решения профессиональной задачи, отражает выбранный компетентностный подход с активной профессионально-производственной подготовкой и сочетанием разнотипных форм обучения.

Сюжет практического занятия:

В ходе разработки Автор написал программу, которая играет сама с собой в жизнь Конвея (http://ru.wikipedia.org/wiki/Жизнь_(игра)). К глубочайшему сожалению Автора, часть файлов затёрлась, а именно ключевая часть программы, где реализованы 4 важные функции. Автор не помнит, что это за функции, и как они работали. Задача обучаемых: восстановить утерянные куски кода.

Рассматривается пример работы рабочей программы, исходный код, работа программы и входные условия сопровождаются комментариями и сервисными навигаторами. Обучающая часть включена в сервис и комментарии и содержит определения, рассматриваемые в лекционном материале: компьютерная программа, процесс, потоки выполнения, точка входа в программу.

Сервисные комментарии сопровождают порядок использования рабочих символов программы: фигурные скобки для группировки, обозначения начала и конца функции, точка с запятой после каждого оператора языка с дополнительными функциями возврата значений, циклов и завершения программы, циклы и блоки кода, предусловия и постусловия выполнения циклов, синтаксис операторов цикла, понятие пустых операторов, области видимости переменной, глобальные и локальные переменные, понятия перекрытия имён глобальной и локальной.

В теле программы разбираются коды, объявленные переменные, их создание и инициализация, операторы ветвления, реализация особых условий выполнения программы, вложенные операторы, введение ограничений. По ходу выполнения программы отмечаются варианты применения других языков программирования и различие применения разных типов данных, возможные последствия перекрытия имён глобальной и локальной переменных.

Весь тематический блок по всем видам учебных занятий заканчивается обязательными вопросами для самопроверки, отражающими знания как теоретические, так и прикладного использования в решении учебных и профессиональных задач:

Что такое операторы ветвления? Назовите их. Какие бывают циклы? В чём их различие? Что такое область видимости переменной? Что такое время жизни переменной и чем она отличается от области видимости?

На примере конкретной практической работы показан шаблон подготовки материала учебного назначения, сочетающий: ознакомительную, повторную и закрепляющий формы; теоретическую и практическую составляющие; теоретический и исследовательский материал; профессионально-ориентированную оболочку подачи материала.

Плотников К.Ю.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

Е-МУЗЫКА: ПОТЕНЦИАЛ ДЛЯ САМОРЕАЛИЗАЦИИ ШКОЛЬНИКА

В докладе представлено видение перспектив и образовательных рисков, связанных с использованием е-музыки, под которой понимается современная цифровая форма бытования собственно музыки с отличающими её особенностями деятельности (процесс её воссоздания, восприятия). Автор выявляет те особенности, которые отличают процесс самореализации школьника через музыку (как коммуникацию, культуру, язык и творчество) в условиях информатизации образования и всё большего распространения музыкально-компьютерных технологий (МКТ). Подчёркивая значение освоения школьником МКТ именно с педагогической поддержкой, автор делает выводы о необходимости отдельного изучения связанных с этим образовательных рисков, а также вопроса художественного репертуара как основы содержания такого образовательного процесса.

Мы предлагаем ввести термин «е-музыка», в котором префикс «е» указывает:

- на особенность данной формы музыки как цифровой;
- а также – на вытекающие из этого особенности деятельности по (вос)созданию и восприятию этой формы музыки, что представлено в процессах: целеполагания, вовлечения, осуществления, анализа и пр., характеризуя взаимодействие актора (если рассматривать данные процессы в категориях социологии) или субъекта образовательного процесса (обучающегося, (само)воспитуемого) с такой музыкой.

Таким образом, стоит признать, что актуальность изучения вопроса самореализации школьника с использованием именно е-музыки обусловлена:

- самой, имеющей место быть (в т. ч. – и среди данной возрастной категории –популярностью музыки во всех её проявлениях (как творчества, как коммуникации, как культуры, как языка);
- что особенно важно, образовательным потенциалом собственно музыки, безусловно, потенциально присутствующем и данной форме её бытования;
- распространившимися с развитием персональной мобильной техники и вошедшими в обиход (включая младших школьников и подростков) технологиями – МКТ;
- теми вызовами со стороны процессов глобализации и информатизации, которые поставлены перед отечественным образованием и связаны с задачей сохранения национальной самоидентификации (к примеру, в разработке методики и отечественного ПО и др.;
- тем противоречием, которое может быть представлено через термин «е-музыка», заключённое, с одной стороны, в наличии данной специфичной формы, с другой стороны, – отсутствием педагогического осмысления её значения, методики её применения и т. д.

Наличие проблемы (поиск решения которой выдвинут нами в качестве цели), состоящей в изучении условий, а также – возможных и реализуемых направлений самореализации школьника с использованием е-музыки, обусловило задачи исследования:

- отбор материалов теоретического и практического изучения данного вопроса в различных его аспектах;
- выбор методов исследования и подходов, способных отразить особенности объекта (самореализации школьника) и предмета исследования (использование при этом е-музыки);
- оценка собранных (в ходе данного и предварительных этапов) результатов;
- формулирование выводов по результатам анализа.

Погодин А.В., Погодина Ю.А., Голомолзин Р.С.
Россия, г. Москва, Технологический университет
Санкт-Петербург, ООО «Центр образовательных проектов и консалтинга «РАДУГА»

ИНФОРМАЦИОННАЯ СРЕДА УЧЕБНЫХ УЧРЕЖДЕНИЙ И ЕЕ ИНТЕГРАЦИЯ С ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Одной из главных задач автоматизации деятельности учебных учреждений является возможность создать единую информационную среду, связав стандартный функционал учетных систем с практической деятельностью учреждения, а также интегрировать в единую базу данных специализированные участки (электронное тестирование, электронная библиотека и т.д.). Подобная схема организации информационной среды будет отражать все основные функции с точки зрения автоматизации процессов управления образовательной деятельностью.

Информационная среда должна распространяться на все представительства, филиалы, а так же объединять отдельные юридические лица или внутренние подразделения как высшего так и среднего профессионального образования.

Отдельные блоки задач формируют части информационного пространства, которые редко удается интегрировать друг с другом. Важным вопросом, создающим дополнительные

информационные потоки, стоит интеграция с внешними информационными системами федерального и регионального уровней.

Для нахождения ответов на эти вопросы информационная среда должна быть построена на единообразной основе из блоков со следующими опорными функциями:

– Блок «Приемная комиссия» должен опираться на формирование единых справочников по набору в ВУЗ и СУЗ, формировать план приема и правила приема, регистрировать заявления абитуриентов, формировать списки абитуриентов, контролировать вводимую информацию; учитывать результаты вступительных испытаний; обеспечивать автоматизированное взаимодействие с ФИС ГИА и приема для ежедневной синхронизации данных о ходе приемной кампании, автоматизированное получение данных ЕГЭ из базы ФБС; формировать оперативную отчетность о ходе приемной кампании; формировать информацию о работе приемной комиссии для публикации на web-сайте учреждения; реализовывать web-кабинет абитуриента.

– Блок «Студенческий контингент» должен автоматизировать формирование и печать приказов по студенческому контингенту; вести историю движения обучающегося и воинский учет обучающихся; содержать большое количество отчетных форм (Формы ВПО-1, СПО-1 и т.п.) по движению студенческого контингента; осуществлять учет договоров и начислений оплаты за обучение, учитывать назначение и расчет стипендии.

– Блок «Учебные планы» должен реализовывать поддержку всех образовательных стандартов; формировать рабочие учебные планы на весь период обучения, с возможностью ведения новых редакций; формировать основные образовательные программы ООП с просмотром текста документов.

– Блок «Учебная нагрузка» должен связывать учебные группы и дисциплины с аудиторным фондом; формировать справочник видов учебной нагрузки с нормами времени и алгоритмами расчета нагрузки; рассчитывать плановую и фактическую нагрузку по кафедрам; готовить информацию для составления учебного расписания; планировать штатное расписание по профессорско-преподавательскому составу.

– Блок «Успеваемость» должен учитывать успеваемость по формам итогового контроля, в том числе с применением балльно-рейтинговой системы оценки знаний; формировать электронное портфолио обучающегося.

В современных условиях автоматизация каждого из этих блоков часто происходит самостоятельно, что приводит к множественному дублированию информации в различных информационных системах учреждения. Это в свою очередь ведет к увеличению затрачиваемых на сопровождение сил и средств.

В условиях ограниченных ресурсов выгоднее использовать единую платформу для нормативно-справочной и учетной информации. Информация, получаемая из такой среды, будет иметь единый источник и не будет давать расхождения при сдаче отчетности во внешние информационные системы федерального уровня, такие как ФИС ГИА и приема. А также снизит затраты на синхронизацию сведений внутри учебного учреждения.

Анализ дублирования информации и процессов синхронизации может дать отправные точки для поиска избыточности в информационных системах. У информационной среды учебного учреждения появится возможность перестать быть «лоскутной» и бесшовно интегрироваться с внешней средой. Удобство использования такой среды студентами, преподавателями и администрации учебного учреждения принесет как финансовый, так и репутационный положительный эффект.

Попова Е.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

МЕТОД ЭКСПЕРТНОЙ ОЦЕНКИ ДЛЯ ФОРМИРОВАНИЯ ИЗМЕРЕНИЙ ПРИ МНОГОКРИТЕРИАЛЬНОМ ВЫБОРЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Современные угрозы информационной безопасности заставляют предприятия обеспечивать защиту информационных ресурсов, не только для сохранения нематериальных активов предприятия, но и соответствия современным законодательным актам в области защиты информации. Одно из эффективных решений заключается во внедрении наилучшего варианта системы защиты информации для данного предприятия.

Задача многокритериального оценивания системы защиты информации при выборе оптимизационного варианта для конкретного предприятия, усложняется условиями, когда критерии равнозначны, независимы и максимально характеризуют состояние изучаемого объекта. Оперирование доминирующим критерием и уменьшение значимости остальных приводит к тому, что результаты измерений не соответствуют принятой точности решения.

Модифицированный многокритериальный метод рандомизированных сводных показателей позволяет получить интегральные показатели, опираясь на которые, возможен выбор оптимального

варианта системы защиты информации. В качестве характеристик рассматриваемых систем используются экспертные оценки коэффициента уменьшения ущерба по нескольким критериям.

При использовании лингвистических шкал и сопоставление их с числовыми, полезно применение аппарата нечётких множеств. Функции принадлежности более эффективно помогают решать задачи перевода лингвистических, вербальных оценок в точные и справляться с трудностями дефазификации.

Фиксирование экспертных оценок в виде треугольных или трапецеидальных нечётких чисел приводит к необходимости выбора метода дефазификации. Для нахождения среднего значения нечёткого числа прибегают к композиции его величин. Оценка $k-го$ коэффициента $m-ой$ системы защиты информации представляется в виде нечёткого числа, определённого на интервале $[0;1]$ и описывается соответствующей функцией принадлежности.

Экспертные оценки используются при выборе одного варианта из нескольких объектов. Метод экспертных оценок представляет собой метод организации работы экспертов и дальнейшей обработке полученных данных. Используются лингвистические, вербальные ранговые шкалы. В толковом словаре Ожегова говорится, что «эксперт (от латинского expertus - опытный, знающий, сведущий) - специалист, дающий заключение при рассмотрении какого-нибудь вопроса».

Эксперты должны обладать следующими качествами:

- компетентность;
- опытность;
- иметь учёную степень;
- эрудированность в смежных областях;
- объективность.

Эксперты должны пройти инструктаж, определить степень согласованности действий. Эксперты получают шкалу измерений, объект измерений, узнают, какое значение показателей является наилучшим. Выводы экспертов должны быть инвариантны относительно допустимых преобразований шкал измерений.

Подбор экспертов может быть основан на коэффициенте согласованности Кендалл-Смита, коэффициенте профессиональной перспективности. Каждому эксперту присваивают весовые коэффициенты квалификации, которые основываются на самооценке и взаимооценке.

Немаловажным является вопрос количества экспертов. С одной стороны с ростом числа экспертов точность измерений возрастает. С другой стороны для минимизации расходов и ограниченности выборки экспертов их число желательно минимизировать. В качестве компромисса можно взять такое количество экспертов n , при котором разница между рассеянием результатов оценок для n и $n+1$ экспертов незначительна.

Грамотно и аккуратно используя метод экспертных оценок при многокритериальном оценивании систем защиты информации, можно прийти к более точным и эффективным расчётам, получить вариант системы, который будет соответствовать максимальным критериальным показателям и выполнять первоначальные цели, поставленные перед системой защиты информации.

Смолина Е.В.
Россия, Санкт-Петербург, Президентская библиотеки имени Б.Н. Ельцина

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ РЕСУРСОВ НАЦИОНАЛЬНЫХ БИБЛИОТЕК В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ (НА ПРИМЕРЕ РАБОТЫ С ЧИТАТЕЛЯМИ БИБЛИОТЕКИ КОНГРЕССА)

Перспективным направлением развития библиотек сегодня становится освоение ими электронной среды, создание национальных электронных коллекций, работа с которыми приведет к эпохе Нового Просвещения, поскольку создаются беспрецедентные возможности для просветительской и образовательной деятельности библиотек. Электронная среда вносит много нового в деятельность национальной библиотеки. Прежде всего, это связано с тем, что в электронной среде у библиотек появляются новые свойства, такие как возможность создавать «комплексный ресурс», формировать «целостные коллекции», обслуживать значительно большие читательские аудитории, а также индивидуализировать свои сервисы.

Сегодня все крупные электронные национальные библиотеки за рубежом имеют сервисы по предоставлению первоисточников, активно включаются в обслуживание образовательной деятельности. В России эта задача также считается приоритетной. Реализация этой задачи тесно связана с библиотечным обслуживанием такой читательской группы как учителя, которая становится одной из основных целевых групп национальных электронных библиотек.

Библиотечное обслуживание учителей строится на идее, что внедрение в образовательный процесс национального наследия, особенно первоисточников является важной составляющей в формировании мировоззрения школьников, воспитании патриотизма, становлении гражданина своей страны.

Национальные электронные библиотеки в мире уже накопили значительный опыт такой работы.

В докладе рассматривается работа с учителями в электронной среде такой крупнейшей библиотеки мира как Библиотека Конгресса США. Она предлагает учителям специальный модуль, который включает учебные материалы и поддерживает профессиональное развитие учителей, помогая им эффективно использовать первоисточники из огромного цифрового контента библиотеки в учебном процессе.

Ресурс, адресованный учителям, начинается с двух Введений, которые называются «Зачем использовать первоисточники?» и «Как использовать первоисточники?». Под «первоисточниками» (primary sources) здесь понимаются любые документы и предметы, созданные в конкретное историческое время, в отличие от «вторичных источников» (secondary sources), которые содержат исследования, интерпретации событий, но сами не являются современниками исторических событий.

Главная страница модуля для учителей включает следующие разделы: 1. Учебные материалы; 2. Профессиональное развитие; 3. Обучение с использованием первоисточников; 4. Использование первоисточников; 5. Новости и события; 6. Дополнительные ресурсы; 7. Ответы на наиболее часто задаваемые учителями вопросы об использовании материалов на их странице. А также на главной странице вход в специальный «Блог для учителей: «Обучение вместе с Библиотекой Конгресса», который ведут библиотечные специалисты. Это – диалог с учителями по раскрытию фондов Библиотеки Конгресса для учителей.

В докладе рассматривается один из семи разделов модуля для учителей: раздел «Учебные материалы» – это методические разработки уроков, предлагающие удобные способы включения первичных источников Библиотеки Конгресса в учебный процесс.

На примере работы Библиотеки Конгресса с учителями как целевой группой пользователей, показано, что работа с читателями национальных библиотек, перемещенная в электронную среду открывает беспрецедентные возможности для обслуживания образовательного процесса, внедрения в обучение уникальных первоисточников, которые делают более эффективным процесс образования, изучения учащимися истории своей страны. Разработка и методическое сопровождение использования первоисточников учителями на уроках гарантирует их высокую востребованность и эффективность. Модуль для учителей – это один из продуктивных направлений продвижения национального наследия, создает равные условия для подготовки учащихся, независимо от места их проживания. В создании раздела модуля «Учебные материалы» и в подготовке методических материалов участвовало более 300 учителей.

Советов Б.Я., Касаткин В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ФУНДАМЕНТАЛИЗАЦИЯ И ПРОФЕССИОНАЛЬНАЯ ОРИЕНТАЦИЯ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

До настоящего времени основной проблемой подготовки кадров остается проблема адаптации выпускника вуза к реальным условиям производства. Сама идеология построения федеральных государственных образовательных стандартов, если не предпринимать специальных усилий, направленных на актуализацию содержания образовательной программы, закладывает риск отставания уровня подготовки кадров на период, соответствующий сроку обучения выпускника. Рассматривается два возможных направления выхода из указанной ситуации.

Первое заключается в повышении уровня фундаментализации образования с профессиональной ориентацией выпускника, определяемой возможностями вуза и заинтересованных предприятий с ориентацией на то, что при серьезной фундаментальной подготовке выпускник самостоятельно получит необходимые умения и навыки в начальный период работы на предприятии. Эта схема наиболее проста для реализации вузами, но предъявляет особые требования к способностям и возможностям самообразования молодых специалистов. Вуз должен при этом обладать значительными ресурсами для организации самостоятельной научно-исследовательской деятельности студентов в рамках студенческих научных обществ.

Второй подход может быть реализован на основе использования опыта советской высшей школы, когда значительной время подготовки кадров было уделено профессиональной ориентации выпускника. В современных условиях реализация этого подхода требует серьезной государственной поддержки как вузов в части финансирования научно-исследовательских работ, так и производственных предприятий, в бюджете которых отдельной строкой должны быть предусмотрены средства на развитие совместных научно-исследовательских работ с привлечением вузов. Предприятие, организуя производственную и иные виды практик студентов, активно участвуя в определении тематики и руководстве выпускными квалификационными работами, привлекая студентов к решению приоритетных научно-производственных задач, могут отбирать для последующей работы и адаптировать студентов к будущей деятельности в период их обучения в

вузах. Указанный подход позволяет реализовать не только инженерную подготовку, но и помочь вузам с выбором тематики магистерских диссертаций и тем самым поднять качество образования.

Организационные формы сотрудничества вуза и промышленного предприятия, вуза и научно-исследовательского института весьма многообразны на практике, но достаточно трудно реализуются в правовом поле, в том числе зачастую по причине отсутствия экономической заинтересованности предприятий. Как следствие, – снижение уровня трудоустройства выпускников по специальности, неоправданное расходование средств на второе высшее образование, дополнительное образование (профессиональную переподготовку и повышение квалификации молодых специалистов) в размерах, превышающих необходимый уровень.

В докладе обсуждаются практические аспекты и многолетний опыт реализации указанных подходов при подготовке разработчиков информационных систем и технологий. Делается вывод о необходимости реализации эффективной государственной политики, направленной на поддержку формирования предприятиями заказов на выпускников и осуществления их отбора в процессе обучения в вузе, что позволит существенно сократить время адаптации специалистов к условиям производства, а также способствовать совершенствованию механизмов регулирования рынка труда и повышению конкурентоспособности отечественных предприятий.

Советов Б.Я., Касаткин В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РОЛЬ АСПИРАНТУРЫ КАК ТРЕТЬЕЙ СТУПЕНИ ВЫСШЕГО ОБРАЗОВАНИЯ ИТ-СПЕЦИАЛИСТОВ

Исторически аспирантура, являлась организационной основой подготовки кадров высшей квалификации как неотъемлемого элемента сохранения и развития научно-педагогических школ в высших учебных заведениях и научно-исследовательских институтах, развивающих актуальные направления научных исследований, способствовала формированию и обновлению интеллектуальной научно-технической элиты общества. Аспирантура, которую всегда относили к научным структурам как в организационном, так и в содержательном плане, оправдывала зарекомендовавшую себя систему: «учитель – ученик», в значительной мере способствовала развитию научно-педагогических школ, определяющих уровень общественного развития.

Требование завершения обучения в аспирантуре в виде защиты диссертации на соискание ученой степени кандидата наук и даже плановые цифры выпуска в аспирантуре способствовали интенсификации научно-исследовательских работ, возникновению новых научных идей и решений, подтверждению их публикациями, монографиями, изобретениями и открытиями. Без сомнения, это способствовало сохранению и развитию интеллектуального потенциала страны, ее приоритета в мировом научном сообществе. Перевод аспирантуры в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ в третью ступень многоуровневой подготовки способствовал превращению аспирантуры в учебную структуру, что естественно повлекло за собой перенос акцентов с мотивации познавательной деятельности, стимулирования творческой активности аспиранта, проводящего научные исследования, на работу по выполнению требований учебного плана, учебных программ, интенсивное участие в учебном процессе, отвлекающим аспиранта от научных исследований.

Закономерным следствием этого явилось снятие требования защиты диссертации по окончании аспирантуры, о чем аттестационная комиссия принимает формальное решение на основании результатов итоговой (государственной) аттестации. Это привело к неопределенности целевого назначения (миссии) аспирантуры, падению ее престижа и частичной потере места в логической структуре системы подготовки кадров.

Все это определяет острую необходимость безотлагательного пересмотра идеологии назначения аспирантуры и определения ее как научной структуры, нацеленной на самостоятельное выполнение аспирантом законченного научного исследования, написание диссертационной работы и последующей защиты ее в определенные временные сроки под руководством научного руководителя.

В настоящее время можно констатировать резкое снижение количества защит диссертаций, поскольку молодые ученые не видят возможности и перспективы реализации своих интересов и способностей в рамках существующего статуса аспирантуры. Что не менее важно, указанный подход способствовал разрушению научно-педагогических школ. Практически исчезла идеология и структура подготовки научных кадров, которые пополняли существующие и вновь создаваемые научно-педагогические школы. Вместо показателей развития научно-педагогических школ значимость в отчетности вузов приобрели индексация научных трудов в зарубежных изданиях, что в ряде случаев может противоречить национальным интересам страны и приводить к навязыванию западных тупиковых стандартов.

В докладе на основе анализа содержания подготовки кадров высшей квалификации в структуре укрупненной группы специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника» обсуждается роль аспирантуры как третьей ступени высшего образования ИТ-специалистов. Делается вывод о необходимости законодательного определения аспирантуры как научной структуры, в рамках которой будут созданы условия, позволяющие аспиранту при резком сокращении учебного процесса полноценно заниматься научной деятельностью с требованием последующей защиты диссертации. Это будет несомненно способствовать возрождению роли научно-педагогической школы, что было и должно оставаться основой инновационного развития Российской высшей школы.

Тен Э.С.
Россия, Санкт-Петербург, Академическая гимназия № 56

МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ НА УРОКАХ МУЗЫКИ В ОБЩЕОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ: ИЗ ОПЫТА РАБОТЫ В АКАДЕМИЧЕСКОЙ ГИМНАЗИИ № 56 г. САНКТ-ПЕТЕРБУРГА

Приобщение современного школьника к вопросам музыкального искусства происходит в условиях чрезвычайно насыщенной среды. Меняется восприятие ребенка, он живет в мире технологичных символов и знаков, в мире электронной культуры. И потому учитель должен быть вооружен современными методиками и новыми образовательными технологиями, чтобы общаться с ребенком на одном языке. И одной из таких методик сегодня является интеграции медийного образования в систему работы учителя-предметника. Научить ребенка ориентироваться в «электронной среде», приобретать навыки «чтения», переработки и анализа информации, получаемой из разных источников, критически осмыслять ее – это и есть одна из важнейших задач современной школы.

В современной школе учитель музыки должен владеть не только музыкально-исполнительскими навыками, но и обладать высоким уровнем профессиональной компетенции, умением руководствоваться имеющимися в его арсенале знаниями в реальной ситуации; быть профессионально мобильным.

Двадцать первый век - это век информационных технологий. Информационные технологии сейчас активно внедряются в различные сферы жизни, среди них и народное образование. В настоящее время большое количество информационных технологий применяется в учебном процессе. Использование информационных технологий в образовательном процессе дает учителю большие возможности при проведении урока, делает урок более увлекательным, запоминающимся, наглядным, позволяет по-новому использовать на уроках музыки текстовую, звуковую, и видеоинформационную часть, обогащает методические возможности урока музыки, придают ему современный уровень. На уроке музыки, использование информационных технологий решает ряд важнейших задач, прежде всего-это повышение интереса к музыке и к учебно-познавательной деятельности на уроке, способствует усвоению учебного материала, активизации познавательной деятельности, реализации творческого потенциала учащихся.

В последние годы при изучении музыки в общеобразовательной школе все чаще используется компьютерная техника, поэтому мы можем значительно обогатить методические возможности урока. Информационные технологии позволяют по–новому использовать на уроках музыки текстовую, звуковую, графическую и видеоинформацию и ее источники – т.е. обогащают методические возможности урока музыки, придают ему современный уровень.

Урок с использованием компьютера, в отличие от традиционного, подразумевает иную организацию: акцентом в представлении и изучении данной темы является непосредственная связь с жизнью. Задания носят конкретный характер. Целью является привлечение детей к самостоятельному изучению предмета, развитие умения ориентироваться в широком объёме информации, анализирование и выделение существенного, важного для всех участников учебной деятельности.

К настоящему времени ГБОУ «Академическая гимназия №56» Санкт-Петербурга - крупнейший в Северо-Западном регионе, образовательный комплекс, основной миссией которого является представление максимального широкого поля возможностей наибольшему числу учащихся, ориентированных на высокий уровень образования и воспитания. Гимназия является одной из лучших школ г. Санкт-Петербурга, которая идет в ногу со временем. Школа соответствует требованиям школы XXI века, все кабинеты оборудованы самой современной компьютерной техникой.

В 2012 г. на базе нашей школы был открыт Музыкально-компьютерный класс для начальной школы. В 2014 г. такие же классы были открыты в начальной школе и в средней школе. Классы МКТ оборудованы 13 компьютерами с MIDI-клавиатурами и наушниками, проектором и smart-доской. Образовательная программа класса МКТ построен на основе Инновационного учебно-методического комплекса «Музыка и информатика» Горбуновой И.Б., Демидов М.В., Чибирев С.В. Также

определённые навыки работы были приобретены в процессе обучения по программе профессиональной переподготовки «Методика преподавания музыкальных дисциплин с использованием музыкально-компьютерных технологий» в Российском государственном педагогическом университете им. А.И. Герцена.

Титова Ю.Ф.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ОБ ОСОБЕННОСТЯХ ТРУДА ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Во ФГОС ВО законодательно закреплено требование к вузам использовать в учебном процессе электронную информационно-образовательную среду и формировать портфолио обучающегося в том числе и в электронном виде. Реализация этого требования проводится путем внедрения в вузах систем управления образовательным контентом (LMS), в которых преподаватели должны выкладывать свои учебные материалы в электронном виде, проверять прикрепленные обучающимися работы, вести контроль знаний, выставлять оценки. Использование в учебном процессе электронного обучения имеет свои положительные стороны. С одной стороны это позволяет получать знания в заочной форме любому желающему, независимо от его местопроживания. Студенты очень хорошо откликаются на такие формы обучения. С другой стороны сильно удешевляет учебный процесс, как известно заочное обучение намного дешевле очного. Вместе с тем закономерно возникает вопрос, связанный с использованием электронного обучения – нормирование трудозатрат преподавателя и оценка в денежном эквиваленте его работы.

Как уже отмечалось МинОбрНауки эти вопросы отдало на откуп вузу, оставив за собой требование – привести зарплату преподавателя к средней по региону. В реальной ситуации вузы до сих пор оценивают работу преподавателя по количеству аудиторных часов. Только если раньше норматив был 600 (доцент) – 720 (ассистент) часов в год, то теперь этот норматив доходит до 900 часов. И это на фоне тотального сокращения в учебных планах аудиторных часов. Оставшиеся 600 часов преподавателю предлагается использовать на разработку электронных материалов, на контроль самостоятельной работы студента, на управление контентом электронной образовательной среде, на научную работу, на воспитательную работу и много еще на что. При организации электронного обучения можно выделить три основных направления работы преподавателя – обучение технологиям работы в среде, создание курса и управление курсом. Создание курса включает в себя разработку конспектов лекций, практикумов, заданий для контрольных работ, и очень трудоемкий и ответственный вид работ – создание тестовых вопросов и тестов для всех видов контроля знаний. Эта работа требует достаточно больших единовременных трудозатрат и трудозатраты на поддержку курса в актуальном состоянии. Другая часть работ – постоянное управление контентом, которое включает следующие трудозатраты преподавателя на 1 дисциплину:

- Запись студентов на курс и удаление с курса;
- Актуализация – связана с удалением старого материала и загрузкой новой версии;
- Проверка выполненных заданий, комментирование результатов проверки;
- Наполнение и актуализация базы тестовых вопросов – связана в основном с наполнением базы, но и с необходимой чисткой;
- Проведение и анализ тестирования (текущего, рубежного, итогового);
- Выставление электронных оценок;
- Индивидуальные консультации;
- Ведение форума;
- И прочие работы.

Для каждого вида работ необходимо выработать критерий оценки и собственно норму, Критерий может опираться в расчете на 1 студента или на группу. Несомненно, трудоемкость должна учитывать общее число зачетных единиц по дисциплине, количество контрольных мероприятий. Чем больше зачетных единиц отведено на дисциплину, тем значимее она при обучении, тем больше ее трудоемкость, как со стороны студента, так и со стороны преподавателя. Число контрольных мероприятий должно увязываться и с формой обучения, т.е. числом аудиторных часов в обратной пропорциональности. Важно не только определить формы и нормы работы преподавателя при использовании электронного обучения, но и обеспечить контроль их исполнения. Для выработки норм необходим мониторинг и экспертная оценка, как преподавателями своей работы, так и администрацией. Если отдельные критерии, так или иначе, подлежат нормированию, то такой вид работ как актуализация нормировать очень трудно. И здесь может придти на помощь практика, которая давно уже применяется для определения гонорара в творческих профессиях – авторские отчисления за использование объекта искусства. Как известно, если запись песни исполняется по радио, то артист получает авторские отчисления. Чем больше она исполняется, тем больше автор зарабатывает. С точки зрения электронного обучения – это могла бы быть оценка стоимости курса в часах, умноженных на количество обучающихся на курсе. Но эта оценка должна опираться на

экспертную оценку авторства при создании курса. Именно потому, что до сих пор не сделана оценка трудоемкости работ преподавателя при использовании электронного обучения, полноценное использование LMS в вузах является уделом преподавателей-альтруистов.

Товпич И.О.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРЕПОДАВАНИИ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН

Современное образование стремительно набирает скорость в области новейших ИТ. В настоящее время современные ИТ занимают определенное место в качественном и эффективном преподавании учебных предметов. Информатизация стала одним из главных направлений получения знаний учащимися в различных предметных областях, в том числе и таких как «Музыка». Практика показала, что процесс обучения с привлечением ИТ на занятиях музыкально-теоретических дисциплин имеет бóльшие возможности и широкие перспективы среди большого количества разнообразных методик. Использование современных ИТ на уроках сольфеджио, теории музыки, музыкальной литературы в ДМШ и ДШИ, а также на уроках музыки в общеобразовательных школах, делает обучение ярким, запоминающимся, интересным для учащегося любого возраста, формирует эмоционально положительное отношение к предмету. Кроме того, учебным планом предусмотрены 1–2 часа в неделю, что явно недостаточно. В связи с этим возникает проблема повышения интенсивности урока, его насыщенности.

Одним из способов решения этой задачи могут стать современные ИТ, которые становятся доступными при использовании интерактивного устройства MIMIO и, несомненно, помогут более эффективному усвоению музыкального материала, повышению интереса к уроку, воспитанию художественного вкуса, развитию творческих способностей, эмоционального отклика учащихся. Использование современного интерактивного оборудования MIMIO позволяет включить не только дидактический и иллюстративный материал, который рекомендован Программами, но и дополнительные аудио- и видеоматериалы. Помимо оригинальных возможностей для закрепления для понимания текущего материала терминологии важны листы/слайды MIMIO. Они позволяют организовать также тестирование, что многократно реализовано в данной работе, являясь не только лишь иллюстративным дидактическим материалом, а дает преподавателю возможность проведения занятий с использованием интерактивного оборудования на современном уровне, когда каждый музыкальный инструмент снабжен иллюстрацией, аудио файлом с рассказом об инструменте и аудио характеристикой звучания. Мы убеждаемся, что интерактивные технологии открывают простор для методического творчества педагога и активных форм усвоения материала для учащегося. Так, например, интересный опыт работы с детьми дошкольных учреждений был представлен на IV Международной научно-практической конференции «Современное музыкальное образование – 2015». Для интерактивных проектов, созданных с использованием технологий MIMIO, были сконструированы модели, развивающие голос, звуковысотность, дыхание, пение в форме канона, мелодическую импровизацию. Всё это сопровождается передвижением и одновременным озвучиванием предметов на картинке, цветных линий маркера, клонированных букв, синхронно передвигающихся с мелодией голоса ребёнка. Одновременно решаются следующие дидактические задачи: координация речи и согласованное движение пальцев рук, развитие быстроты реакции, артикуляционной моторики, активизация восприятия, развитие слухо- двигательной и тактильной памяти, воспитание отношений партнёрства, плавности речевого выдоха, развитие чувства темпа, развитие коммуникативных навыков, развитие зрительно-моторных координаций, развитие саморегуляции мышечного тонуса, воображения.

Устюгова Т.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

СЕТЕВЫЕ СЕРВИСЫ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ В ПОДГОТОВКЕ БАКАЛАВРОВ ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ

В условиях информационного общества и глобальной информатизации различных областей жизни выпускники высших педагогических учебных заведений должны быть готовы изучать и разрабатывать, оценивать и внедрять новые электронные образовательные ресурсы (ЭОР), позволяющие обогащать информационную образовательную среду школы и вуза.

Анализ научно-педагогической, методической, учебной литературы, практики использования ЭОР в образовании показывает, что необходимо формировать у будущих педагогов компетенции, которые позволили бы разрабатывать качественные ЭОР, затрачивая оптимальное время и уделяя внимание качеству реализации и содержательному наполнению.

На наш взгляд, соответствующие компетенции связаны с развитием медиакомпетенции педагога, под которой будем понимать готовность создавать и редактировать мультимедийные

образовательные ресурсы, включающие графику, анимацию, аудио и видео фрагменты, инфографику и текст с использованием средств информационных технологий.

Для оценки сформированности медиакомпетенций у обучающихся на основе проведённого анализа литературы, был использован подход А.В. Фёдорова, базирующийся на следующих критериях: информационный, перцептивный, интерпретационный, мотивационный и контактный. Набор лабораторных работ и электронная образовательная среда могут использоваться как учебный модуль, который можно использовать в рамках аудиторной работы в дисциплинах методического цикла или для самостоятельной работы студентов.

В целях развития медиакомпетенций будущих педагогов мы отобрали набор сетевых сервисов, разработали комплекс лабораторных работ по их освоению, включающие теоретический материал, упражнения, и тестовые задания. Для повышения наглядности обучения были разработаны разнообразные материалы для демонстрационных примеров. В комплекс лабораторных работ используются сервисы для обработки мультимедийной информации pixlr.com, sumopaint.com, mp3cut.ru, youtube.com, easel.ly, multator.ru, ilovepdf.com, prezi.com. Критериями отбора были выбраны следующие: аналог профессиональных средств, свободное распространение, актуальность, обновляемость, востребованность, возможность использования для решения широкого круга профессиональных, учебных и повседневных задач в образовании.

Для управления учебной деятельностью, в том числе в дистанционной форме, был разработан фрагмент информационной образовательной среды, включающий сайт, содержащий комплекс лабораторных работ и позволяющий пройти тестирование по итогам выполнения контрольных заданий в тестовой форме; группу коммуникационной поддержки «ВКонтакте», в которой обучающиеся имеют возможность разместить выполненные индивидуальные проекты, взаимодействовать друг с другом и преподавателем, оценить проекты других участников группы. Кроме того, преподаватель публикует итоговую таблицу с результатами выполненных итоговых заданий.

Для апробации результатов обучения было проведено экспериментальное исследование, в котором приняли участие бакалавры педагогического образования, профиль «Информатика и информационные технологии в образовании» 1-3 курсов РГПУ им. А.И. Герцена. В ходе исследования были определены начальный и итоговый уровни сформированности медиакомпетенции обучаемых после завершения обучения в модуле.

В начале эксперимента выявлена сформированность медиакомпетенций у обучающихся по критериям: информационный – средний (55%), перцептивный – низкий (35%), интерпретационный – низкий (37,75%), мотивационный – высокий (75,5%), контактный – средний (47,2%). По результатам обучения были зафиксированы следующие результаты: информационный – высокий (73%), перцептивный – средний (45%), интерпретационный – средний (47%), мотивационный – высокий (80%), контактный – средний (55%). Значения уровней указаны из расчёта: 0-40% - низкий уровень показателя, 40-70% - средний уровень, 70-100% - высокий уровень.

Заключение. Эксперимент показал рост уровней по всем показателям развития медиакомпетенций, в том числе значительное сокращение времени на выполнение индивидуальных проектов.

Фатьянова Е.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ПЕРСПЕКТИВЫ ОБУЧЕНИЯ ИГРЕ НА СИНТЕЗАТОРЕ В СИСТЕМЕ СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ

В настоящее время обучение игре на синтезаторе в системе среднего специального образования не распространено. На мой взгляд, необходимо знакомить будущих музыкантов-профессионалов с техническими возможностями электронного музыкального инструментария и демонстрировать варианты применения уникальных современных технологий для воплощения художественного образа.

В современном музыкальном образовании существует несколько вариантов применения электронного музыкального инструментария: исполнительское мастерство с изменением параметров в реальном времени с помощью контроллеров, искусство аранжировки, ансамблевое исполнительство, в том числе с акустическими инструментами и вокалом, создание авторских сочинений и мультимедийных проектов.

Благодаря синтезатору в системе среднего специального образования возможно взаимодействие и углубление межпредметных связей. Для обучения игре на электронном музыкальном инструменте необходимы знания в области элементарной теории музыки, гармонии, анализа музыкальных произведений, оркестровки, инструментовки, изучение музыкальных шедевров композиторов прошлого и современности. В свою очередь углубленное изучение синтезатора обогащает деятельность будущего музыканта знаниями в области применения современных способов обработки и синтеза звука, создания оригинальных стилей. Несомненно, многотембровость

инструмента расширяет кругозор, способствует развитию тембрального слуха, что необходимо для создания оригинальных аранжировок, сочинения музыки для театральных постановок, телевидения и радио, реализации уникальных проектов в области звукового дизайна.

В результате данных преобразований деятельность музыканта-аранжировщика, композитора, звукооператора, исполнителя становится более продуктивной, эффективной, качественной.

Дальнейшее развитие и совершенствование системы образования призвано формировать универсального специалиста с большим багажом знаний и практических навыков, воспитывать музыканта будущего, обогащая традиционное образование современными технологиями.

Хомутская Н.Ю.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Детская школа искусств Красносельского района

ИМПРОВИЗАЦИЯ НА ЭЛЕКТРОННЫХ МУЗЫКАЛЬНЫХ ИНСТРУМЕНТАХ

Мы находимся в поле информационных технологий музыкального образования. Активное развитие данного направления в последние годы и решения разнообразных задач не могли не затронуть и музыкальную среду. В современном музыкальном образовании вопрос обучения основам импровизации на электронных музыкальных инструментах затрагивается достаточно часто. Таким образом, внедрив этот образовательный элемент, мы можем раскрыть новые возможности музыкального инструментария не только с их технической стороны, но также и с художественной. Импровизация – как основной элемент раскрытия индивидуальных возможностей исполнителя, который одновременно становится создателем чего-то прекрасного и неповторимого.

Музыкальная импровизация – как фундамент и важнейший элемент завоевания новой высокотехнологичной информационной образовательной среды. Музыкальная импровизация – как одна из ярких возможностей соединения музыканта и художника, создателя и исполнителя. Необходимо создавать новые алгоритмы творческой работы музыканта – исполнителя на электронных музыкальных инструментах (ЭМИ), изучение и освоение всех технических характеристик новых инструментов. Постоянное совершенствование и информационная поддержка музыканта помогает отойти от общепринятых норм музицирования, позволив тем самым создать новое поколение музыкантов. Использование всех технических возможностей ЭМИ, соответствующие настройки контроллеров управления, воспроизведение заранее подготовленных музыкальных этюдов, создание каждый раз новых вариантов импровизаций позволяет рассматривать импровизацию на ЭМИ как новый способ трансляции музыкальной культуры в системе современного музыкального образования.

Черний В. Н.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ИНТЕРАКТИВНЫЕ МЕТОДЫ ОБУЧЕНИЯ СТУДЕНТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бурный всплеск мультимедиа породил огромное разнообразие мультимедийных образовательных ресурсов, феноменом для образования в которых была не только высочайшая визуализация обучения, но и в отличие от телевидения и видеоматериалов – интерактивность.

Интерактивный («inter» – это взаимный, «act» – действовать) – означает взаимодействовать, находиться в режиме беседы, диалога с кем-либо. Важное отличие интерактивных упражнений и заданий от обычных в том, что выполняя их, обучающиеся не только и не столько закрепляют уже изученный материал, сколько изучают новый.

Современным студентам требуется, чтобы знания по информационных технологиям преподавались с использованием аудиовизуальных и интерактивных технологий, чтостановится просто необходимым для «погружения» в предмет. С помощью новых технологий возможно не столько увеличить объем образовательнойинформации, сколько при том же самом фиксированном времени «углубиться» в материал, лучшепонять его. К тому же большое значение имеет эмоциональный эффект.

Интерактивное обучение дает возможность сменить стиль и подачу знаний, уйти от традиционных форм обучения и прийти кновым, изменить учебный процесс «изнутри».

Учебный процесс превращается в событие, активное участие, действо для студента. Связь творческого и образовательного процессов с компьютерными и аудиовизуальными технологиями позволяет не просто сделать обучение наглядным, но и достигнуть максимально эффективного диалога между студентом и преподавателем. Интерактивное обучение подразумевает использование следующих технологий:

Все интерактивные методы обучения можно разделить на три большие группы на основаниисред взаимодействия: интерактивные методы обучения в среде «обучающийся –

обучающийся – преподаватель»; в среде «обучающийся – компьютер – преподаватель»; в среде «обучающийся – учебник – учебное пособие».

Наиболее интересным и востребованным в образовательной практике является такой виртуальный учебный объект как интерактивная модель.

Анализ форм взаимодействия пользователя с интерактивной компьютерной моделью позволяет выделить уровни ее интерактивности.

Первый уровень интерактивности. Условно-пассивные формы взаимодействия. Этот уровень характеризируется минимальным взаимодействием пользователя с моделью. Пассивными данные формы названы с некоторой долей условности потому, что от пользователя все-таки требуются некоторые управляющие воздействия (работа с клавишами «пуск», «стоп», «пауза» и т.п.). Цель и требуемый результат работы заранее определены: восприятие и усвоение «готовой» информации.

Интерактивные учебные модели имеют ряд особенностей, которые следует учитывать в реальной учебной деятельности.

Во-первых, активное взаимодействие участников образовательного процесса в учебной деятельности.

Во-вторых, использование интерактивных учебных моделей предполагает следующую логику учебной деятельности: мотивация – формирование нового опыта – его осмысление через применение – рефлексия.

В-третьих, интерактивные учебные модели основаны на игровых формах обучения, при которых проявляется активность обучающихся, осуществляется аккумуляция и передача социального опыта, создаются условия для более полной самореализации личности обучающихся.

С целью повышения эффективности учебной деятельности и содействию самореализации личности обучающихся, преподавателю необходимо свободно ориентироваться в многомерии и многообразии интерактивных учебных моделей, которые являются средством развития профессиональной компетентности студентов в области информационных технологий.

Анализ научной, специальной литературы и обобщение опыта применения интерактивных методов обучения позволяют сделать вывод о том, что их комплексное использование в системе высшего образования является критерием оценки эффективности коммуникативной деятельности обучающихся, а также реализовать основную цель обучения – обеспечить формирование личных и профессиональных компетентностей будущих специалистов в области информационных технологий.

Чёрная М.Ю.
Россия, Санкт -Петербург, Смольный институт Российской академии образования

ФОРМИРОВАНИЕ НОВОЙ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ МЫШЛЕНИЯ СОВРЕМЕННОГО МУЗЫКАНТА

В настоящее время в музыкальном образовании активно развиваются информационные технологии – программные продукты для музыкального творчества, электронный музыкальный инструментарий для исполнителей, интернет-технологии в обучении музыке.

Целью информационного музыкального образования является повышение эффективности учебного процесса, открытие новых возможностей в музыке, а главное, формирование новой информационной культуры мышления музыканта, которая объединяет интеллектуальные возможности человека с информационными технологиями.

Ввиду этого, изменяется сам процесс обучения музыке, теоретические знания из области информационных технологий вводятся в практическую деятельность музыканта, меняется техника исполнительства на электронном музыкальном инструменте (ЭМИ), формируется новый музыкально-компьютерный язык.

Обучение музыке становится интеллектуально-технологическим и основано на интерактивном взаимодействии музыканта (пользователя) с компьютером или ЭМИ.

В свою очередь, информационные технологии не заменяют, а расширяют творческие возможности музыканта, открывают огромные перспективы в освоении новых звучаний, необычных, не встречающихся в природе тембровых сочетаний, а также позволяют трансформировать, моделировать и конструировать музыкальный текст в недоступной прежде звуковой области – звукосинтеза и музыкальной акустике.

Важно отметить, формирование информационной культуры мышления музыканта - процесс сложный, многоуровневый и начинать его необходимо уже в детских музыкальных школах.

Эти задачи наша кафедра «Мультимедиа технологий» решает путем реализации модели непрерывного образования «Школа-колледж-вуз».

Таким образом, интенсивное развитие компьютерного инструментария в музыкальном образовании, появления новых учебных программ, дисциплин, методик указывают на то, что формируется новая информационная культура мышления музыканта, в котором необходимо каждому педагогу грамотно сочетать традиционные музыкальные знания с неограниченными возможностями компьютерных технологий.

Чистякова Т.Б., Новожилова И.В., Полосин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННОГО ОБУЧЕНИЯ СПЕЦИАЛИСТОВ МЕЖДУНАРОДНЫХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Развитие современных производственных технологий требует подготовки нового поколения высококвалифицированных специалистов, готовых к осуществлению профессиональной деятельности на международном уровне и способных своевременно реагировать на новые инновационные технические идеи, способы их внедрения и реализации. Для обеспечения эффективного процесса обучения специалистов промышленных предприятий на рабочем месте актуальным направлением является применение систем электронного обучения, позволяющих с использованием дистанционных образовательных технологий значительно экономить временные и финансовые затраты на обучение специалистов. При этом реализация компетентностно-ориентированных образовательных программ в форме электронного обучения осуществляется с помощью электронной информационно-образовательной среды, включающей в себя электронные информационные и образовательные ресурсы, совокупность информационных и телекоммуникационных технологий, а также соответствующих технологических средств обучения.

Для формирования билингвальной компетентности специалистов международного уровня электронная информационно-образовательная среда включает соответствующее лингвистическое обеспечение образовательной деятельности (тезаурусы и комплекс языковых учебно-методических материалов). Интеграция актуальных и новых знаний в единой образовательной среде позволяет создавать современную базу для изучения инновационных производственных и наукоемких технологий. Содержание билингвального компетентностно-ориентированного обучения специалистов формируется на основе модульной технологии с соответствующим лингвистическим обеспечением образовательной деятельности. Таким образом, имеется возможность формирования индивидуальных образовательных траекторий в соответствии с требованиями профессиональных стандартов для ликвидации квалификационных дефицитов промышленных предприятий.

Наиболее перспективным направлением для освоения компетентностно-ориентированных результатов обучения специалистов промышленных предприятий является создание интеллектуальных компьютерных тренажеров, позволяющих осуществлять изучение современного промышленного оборудования, изучение причинно-следственных связей в объекте изучения, обучение управлению технологическими процессами на базе виртуальных лабораторий и имитационных математических моделей в рамках единой электронной информационно-образовательной среды. Функциональная структура компьютерного тренажера включает модули, выполняющие функции обучения и тренажа: интерфейс инструктора; интерфейс обучаемого; модуль выполнения вычислительных экспериментов; модуль формирования результатов имитационного моделирования; информационное и математическое обеспечение. Разработанные методы и технологии создания тренажеров апробированы и внедрены на ряде ведущих международных корпораций и промышленных предприятий, таких как Klöckner Pentaplast Group, ООО «Вириал», ПАО «Северсталь», ЗАО «ИЛИП», ОАО «АК «Ригель» и др.

При реализации электронного обучения специалистов международных предприятий наиболее сложной задачей является качественная и количественная оценка приобретаемых билингвальных профессиональных компетенций. Для количественной оценки результатов освоения билингвальных профессиональных компетенций используются языковые контрольно-измерительные материалы, комплексные задания (практические или проектные) и выпускные аттестационные работы. Для качественного определения уровня подготовки специалистов используются модели контроля знаний: регистрация полученных знаний, оценка знаний по контекстной модели, анализ ошибок, метод наложения и порождающее моделирование.

По результатам проведения апробаций различных компетентностно-ориентированных образовательных программ для специалистов промышленных предприятий наиболее эффективным средством освоения компетентностно-ориентированных результатов обучения является использование электронной информационно-образовательной среды, позволяющей аккумулировать передовые знания в области современных производственных технологий, повысить уровень безопасности промышленных производств, повысить качество продукции, улучшить экологические характеристики производственной среды за счет повышения профессионального уровня специалистов (приобретения опыта и навыков поведения в аварийных ситуациях, глубокого понимания причинно-следственных связей в объекте, быстрой реакции на неполадки, снижения психологической перегрузки, увеличения уверенности, самостоятельного решения задач управления).

Таким образом, использование современных информационных технологий позволяет повысить профессиональный уровень специалистов современных промышленных предприятий и приблизить их квалификацию к требованиям профессиональных стандартов в условиях полиязычной среды.

Шалаева Е.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ВОЗМОЖНОСТИ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В РАЗВИТИ ОБЩЕКУЛЬТУРНЫХ КОМПЕТЕНЦИЙ СТУДЕНТОВ – БУДУЩИХ ПЕДАГОГОВ

Изучение процесса формирования и развития общекультурных компетенций (ОК) студентов – будущих педагогов является актуальной проблемой отечественных и зарубежных ученых. Радикальные социально-экономические преобразования в российском обществе актуализируют потребность в высококультурном специалисте. В этих условиях происходит смена приоритетов, становится возможным усиление культурообразующей роли образования, появляется новый идеал студента — «человека культуры», обладающего ОК. Именно ОК определяет активную жизнедеятельность человека, его способность ориентироваться в различных сферах социальной и профессиональной жизни, гармонизирует внутренний мир и отношения с социумом. Значимость этого интегративного качества личности повышается также в связи с переходом от традиционной к личностно-ориентированной парадигме образования, когда обществу нужны активные, компетентные специалисты, способные самостоятельно принимать решения и готовые взять на себя ответственность за их осуществление, умеющие ставить цели и конструировать пути их достижения.

Вместе с тем, современный образовательный процесс вуза, где закладываются основы ОК студентов, всё ещё не обладает необходимым потенциалом для решения данной проблемы. Существующие педагогические технологии не способствуют в достаточной степени формированию ОК студентов. Они либо не предполагают постановку данной проблемы в качестве задачи образовательного процесса, либо не относят решение этой задачи к учебной деятельности.

Анализ научных работ показал, что в настоящее время нет единых взглядов на природу феномена «общекультурная компетентность»: не дано универсального определения, нет общепризнанной структуры ОК. Практика свидетельствует о том, что несформированность ОК тормозит личностный рост студентов и влияет на эффективность всего образовательного процесса. Поэтому формирование ОК как интегративного качества личности, определяющего личностный рост студентов и способствующего совершенствованию образовательного процесса в вузе, приобретает особую значимость.

В диссертациях последнего десятилетия раскрыты возможности формирования ОК студентов в образовательном процессе вуза с учетом педагогического потенциала иностранного языка в формировании общекультурной компетентности студентов (Ежова Т.В.), возможности развития ОК средствами музейной педагогики (на примере подготовки будущих педагогов) (Троянская С.Л.), развитие ОК в физкультурной деятельности (Смирнова Е.И.), за полем зрения остается огромная область накопленных человечеством знаний, способных качественно повысить уровень развития ОК через инновационные средства трансляции материала и включения в образовательный процесс современных музыкально-компьютерных технологий (МКТ).

Уникальной в своем роде, имеющей передовой опыт в разработках, опережающих социальный запрос, является Учебно-методическая лаборатория «Музыкально-компьютерные технологии» РГПУ им. А.И. Герцена. Так, коллективом авторов во главе с руководителем и организатором УМЛ «Музыкально-компьютерные технологии» РГПУ им. А.И. Герцена профессором И.Б. Горбуновой была организована и проведена широкомасштабная апробация разработанной комплексной инновационной образовательной системы «Музыкально-компьютерные технологии» в пилотных регионах России, о чём свидетельствуют, в частности, образовательные ресурсы, ЦОРы и ИУМК, находящиеся на открытом доступе в сети.

Шутов И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский техникум железнодорожного транспорта

СЕТЕВАЯ ОБРАЗОВАТЕЛЬНАЯ СРЕДА КАК СРЕДСТВО ФОРМИРОВАНИЯ КОРПОРАТИВНЫХ КОМПЕТЕНЦИЙ

В настоящее время в холдинге «Российские железные дороги» решается проблема повышения эффективности производственных процессов, что немыслимо без расширения зон обслуживания, совмещения профессий, повышения квалификации работников для использования современных технологий во всех сферах создания транспортного продукта и обеспечения транспортных услуг. Требуемые характеристики работников могут быть обеспечены путем формирования и последующего непрерывного развития корпоративных компетенций в системе технической учебы, стажировок, переподготовки, повышении квалификации и т.п. Представляется, что использование высокотехнологичной образовательной среды при взаимодействии участников процесса обучения позволит эффективно формировать и развивать корпоративные компетенции при подготовке персонала 4-го (рабочие и служащие) и 3-го (специалисты и руководители структурных подразделений) уровней корпоративных компетенций.

Дидактический смысл внедрения высокотехнологичной интеллектуальной среды в процесс подготовки и повышения квалификации работников массовых профессий, которые непосредственно взаимодействуют с клиентами железнодорожного транспорта, заключается в обеспечении непрерывной совместной деятельности обучающихся между собой в учебной группе (по горизонтали), с руководителями или подчиненными (по вертикали) и с преподавателями различных курсов. Для этого создаем систему дидактических условий социализации и профессионализации субъектов образовательного процесса на базе использования сетевых ресурсов телекоммуникационного пространства. Виртуальная часть образовательной среды становится не только условием, но и средством деятельности субъектов процесса формирования корпоративных компетенций. В практической работе на базе учебного центра Дирекции скоростного сообщения – филиала ОАО «Российские железные дороги» были использованы научные принципы организации виртуальной сетевой образовательной среды, разработанные коллективом кафедры информатизации образования РГПУ им. А.И.Герцена под руководством профессора Носковой Т.Н.

В современной практике корпоративного образования преобладает односторонний подход, осуществляющийся как воздействия преподавателя без акцентирования своего внимания на запросы обучающихся. Такой подход обусловлен инженерным образованием преподавателей профессионального цикла учебных дисциплин, которые педагогические условия формирования корпоративных компетенций применяют на основании небольшого преподавательского опыта. В связи с чем нами предложено обеспечить взаимовоздействие субъектов образовательного процесса в учебном центре в рамках дистанционной поддержки обучения, когда преподаватель воздействует на образовательную среду учебным материалом, а обучающийся – созданным при обучении продуктом.

Продуктом обучения при этом считаются выполненные промежуточные и итоговые задания, которые должны быть проверены и оценены у каждого обучающегося. В разработанной нами системе выполненные задания выкладываются на страницах блога, комментируются участниками различных ровней обучения и получают интегративную оценку. В популярнейшей социальной сети ВКонтакте действует учебная группа УЭР-ПП (пассажирские перевозки) по протоколу https://vk.com/club5252717. По мере развития субъектных отношений в рамках процесса формирования профессиональных компетенций стали использовать возможности сайта https://sites.google.com/site/rzdfpkinfo, где размещены как информационные и обучающие материалы, так и выполненные обучающимися задания. Сетевое взаимодействие субъектов образовательного процесса существенно активизировалось при общении в ходе выполнения заданий на блоге «Проблемы пассажирских перевозок» https://spb-shutov.blogspot.ru.

Сетевые ресурсы Интернета стали использовать в различных звеньях общего, специального и профессионального образования, поскольку сеть Интернет обеспечивает не только доступ к информации, но и позволяет организовать взаимодействие субъектов образовательной деятельности в глобальной информационной среде. При этом компьютерная сеть используется не только как сеть компьютеров, где размещены информация и сервисы, но и как «сеть людей», глобальная социокультурная среда, в которой представлены индивидуальные пользователи и сетевые сообщества. Подлинное сетевое сообщество возникает при особой мотивации пользователей Интернета, их активности по отношению к ценностно разделяемому ресурсу, друг другу и общей деятельности в информационной среде. В ходе разработки и организации высокотехнологичной сетевой образовательной среды нам стало ясно, что решающее значение приобретают такие характеристики сетевых сообществ как общие цели, интересы, ценности и потребности. Следовательно, в образовательной практике учебного центра нами использованы методологические основания функционирования социальных общностей в сети Интернет как основанные на регулярном обмене информацией средствами коммуникаций компьютерных технологий, что представляется важным средством формирования корпоративных компетенций работников железнодорожного транспорта.

Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИНФОРМАЦИОННЫЙ СЦЕНАРИЙ ПРОИЗВОДСТВЕННЫХ ЗАДАЧ В ПРОФЕССИОНАЛЬНОМ ОБУЧЕНИИ СТУДЕНТОВ

Федеральный государственный образовательный стандарт высшего образования предъявляет обязательные требования к формированию профессиональных компетенций, соответствующих видам профессиональной деятельности, на которые ориентирована программа обучения. Программы бакалавриата и прикладной магистратуры ориентированы на производственно-технологический, практико-ориентированный, прикладной виды профессиональной деятельности как основной и программа академической магистратуры ориентирована на научно-исследовательский и педагогический вид профессиональной деятельности как основной. Независимо от уровня и вида

обучения выпускник высшей школы должен обладать целостным представлением о производственном цикле решения своих профессиональных задач. Направление подготовки информационные системы и технологии позволяет дважды использовать достижения и концепции информационных технологий: как для всех направлений профессиональной подготовки на базе информационных моделей производственной среды, так и на уровне построения информационных моделей, технологий, базы данных - как предмета и объекта изучения.

Для освоения области своей профессиональной деятельности предлагается построение типового информационного сценария производственных задач в общем варианте, включающем основные, характерные и специфичные аспекты профессиональной деятельности. Сценарий включает в себя подборки по типовым профессиональным задачам; технологическим процессам производства; проблемным ситуациям; коммуникативным процессам; инструментальной базе; информационной поддержки; нормативно-правовым требованиям, лицензировании и сертификации, сервисному обслуживанию; методическому и инструктивному сопровождению. В основу сценария положены общие структуры функций специалиста в контексте технологических процессов решения производственных задач, включая постановку задачи, её поэтапное решение; инструментальное оснащение, формулирование ожидаемого результата ее решения.

В учебной деятельности воссоздаются технологические цепочки и процессы профессиональной деятельности в ходе решения моделируемых профессиональных задач. Для активизации профессиональной направленности мышления обучаемого типовые информационные сценарии включаются в дисциплины обязательной базовой части программы, вариативной части, практики по получению первичных профессиональных умений и навыков, практики по получению профессиональных умений и опыта профессиональной деятельности, технологической практики, НИР. Избыточный подход к построению типового информационного сценария позволяет для всех видов учебной нагрузки использовать сокращённые и упрощенные варианты сценариев. Сквозное использование общей концепции формирования профессиональной подготовки нацелено на формирование целостного представления о профессиональной среде: конкретных производственных задачах, средствах и формах их решения, участниках производственного процесса, их распределении по технологическим цепочкам решения частных производственных задач. Предполагается, что типовые информационные сценарии и их распространённость на все виды учебного процесса позволят натренировать профессионально важные качества будущего специалиста для решения широкого круга профессиональных задач и проблем, развить самостоятельный творческий подход, заложить основы последующей профессиональной адаптации и самостоятельно конструируемого опыта в динамически меняющихся технологических и коммуникативных процессах будущего труда, освоить те формы производственных предложений, с которыми придётся столкнуться в реальных производственных условиях профессиональной деятельности.

Для специалистов по информационным системам и технологиям предметом изучения и освоения могут стать сценарии, модели и информационные базы информационного сценария производственных задач, его составные части, конструкции, информационная поддержка. В ходе практических занятий обучаемые могут расширять, дополнять, конкретизировать модели производственного процесса и прикладной области, моделировать производственные задачи на различных исходных данных и параметрах, осваивать различные формы представления результатов, в том числе, с правовой защитой и соблюдением нормативных правил и требований. При этом студент выступает в позиции активного субъекта обучения и обеспечивает проблемную, исследовательскую направленность образовательной деятельности в ходе имитации проектирования и решения профессиональных задач информационных технологий, высвобождает потенциал для освоения меняющихся технологических процессов, применения новой инструментальной и программной базы, вычленяет значимые отношения и устойчивые связи в меняющемся потоке событий, соотносит собственные действия с основным производственным процессом.

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

АВАНГАРД В ИСКУССТВЕ – ПРАКТИЧЕСКОЕ ИЛЛЮСТРИРОВАНИЕ НЕПРОИЗВОЛЬНОГО ВНИМАНИЯ

Систематизация представления данных в искусстве требует научно-обоснованного подхода, это важно для развития теории данного вопроса и улучшения качества художественно-графического образования.

Авангард, являясь "авансом" возможного большего информационного объема, широко представлен в художественном моделировании XX в. Искусство следует рассматривать как отражение субъективного восприятия объективной действительности. Процесс восприятия претерпевает смену состояний, этапов получения и дальнейшей переработки информации, т.е. в норме, всегда есть начало процесса, середина и конец. Первая стадия получения информации, как

первое впечатление, в психологии называется непроизвольным вниманием. И.П. Павлов описал этот процесс как ориентировочный рефлекс. Многие ученые работают в этом направлении. Они определяют огромное количество информации как избыточное и многоканальное, объясняя, что человек выбирает из этой информации более значимые для него сведения для осуществления личностного процесса восприятия.

Непроизвольное внимание в течение, якобы пассивного, созерцания активизируется множеством интересных объектов и явлений в окружающем мире. Включаются механизмы настройки человеческого организма на знакомство с информацией, раздражителями могут стать новые объекты, контрастность, движение, внутреннее состояние и т.д. Начинают работать анализаторы: зрительные, слуховые, обонятельные, осязательные, …, каждый из них состоит из рецептора, проводниковой части и высшего центра в коре головного мозга – группы нейтронов, которые проводят информацию. Впечатления, полученные в результате восприятия, в дальнейшем явятся основой мыслительных и творческих процессов. Человек дает аналитическую оценку полученным сведениям, формирует свое отношение к ним. Судя по изречениям "первое впечатление", "масса впечатлений", впечатление имеет информационный объем и качественные характеристики: "плохое впечатление", "незабываемое впечатление". Так, например, прежде чем композиционно выстроить стихотворение "Лиличка!" Вместо письма (произвольное внимание), В. Маяковский констатирует пережитые им факты непроизвольного внимания: "…В мутной передней долго не влезет, сломанная дрожью, рука в рукав", " Дикий, обезумлюсь, отчаяньем иссечась." Тяжелое душевное состояние автора объясняет сумбурное искажение слов. Также, мы видим искажение лица "Плачущей женщины" Пабло Пикассо, его же "Герника", намеренно, композиционно выстроена в виде сравнительной диаграммы, чтобы показать разрушения и гибель людей.

Авангардисты пишут не академические произведения, а передают свои впечатления и состояния с помощью изобразительных приемов, где трактовки процессов восприятия и передачи информации более скоростные, порой превращающиеся в быстрые сообщения - схемы. Схема как возможность представления данных считается условным графическим изображением, позволяющим в лаконичной форме представить информацию. С той, примерно, разницей с которой короткое сообщение отличается от рассказа или повести, т.е. более логически последовательного и объемного изложения. Например, женские портреты, выполненные Амедео Модильяни, не имеют портретного сходства с натурой, художник не ставил такой цели. Зато, явно ощущается накал страстей и бесконечное тепло, исходящее от его работ. Это помнится еще с выставки Арманда Хаммера, прошедшей в Ленинграде в Государственном Эрмитаже в 1972г.

Произведения Авангарда это – эмоционально окрашенные быстрые, с небольшим информационным объемом, зарисовки-сообщения, которые можно назвать и схемами и диаграммами.

Разнообразие наименований, составляющих "Авангард" и понимание этого вопроса говорит о том, что количество названий внутри "Авангарда" может быть еще большим. Каждый раз, это – новые впечатления, которые можно группировать по содержанию. Терминологические разновидности, не иначе, всего – лишь, – темы. Содержания этих тем подмечены в процессе непроизвольного внимания в разные исторические периоды. Диапазон развития мирового визуального восприятия и представления данных, является экспозицией от негативного отношения к происходящей действительности к позитивному отношению, и наоборот.

Предлагается определение понятию Авангард: представление данных на основе первичного фазового состояния процесса восприятия, иногда вполне достаточного для использования.

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

РЕАЛИЗМ В ИСКУССТВЕ – ПРАКТИЧЕСКОЕ ИЛЛЮСТРИРОВАНИЕ ПРОИЗВОЛЬНОГО ВНИМАНИЯ. РЕАЛИЗМ КАК СТАДИЯ ГОТОВОЙ ХУДОЖЕСТВЕННОЙ ФОРМЫ.

Формирование нового научного взгляда на теоретические проблемы художественно-графического образования востребовано временем. Исторический подход к этому вопросу продолжает оставаться актуальным, но не достаточным. Понятия просветительский, критический, социалистический реализм не дают целостного знания о реализме. Подход к вопросу с точки зрения аудиовизуального восприятия, в последовательности от ориентировочного рефлекса к следующей фазе произвольного внимания и далее ведет нас к новому пониманию решения проблемы и терминологическому порядку.

Восприятие, преодолев начальную стадию непроизвольного внимания, переходит к произвольному вниманию, которое иначе называют селективным. Автор проводит отбор и анализ информации с целью практического применения. Прежде чем перейти в стадию готовой художественной формы, произведение претерпевает несколько этапов подготовки, это - пристальное изучение исторических фактов, натуры, эскизы, наброски, композиционно-графические варианты,… В процессе работы художник постоянно уточняет изображение, в соответствии со своим авторским

замыслом, стремясь максимально приблизиться к объективному отражению сюжета. Творческая работа предполагает рассмотрение будущей художественной формы с максимально возможных точек зрения. Поэтому количество параметров (информационных величин), образующих искомую модель, по возможности – максимально; соответственно, увеличивается количество фаз по образованию сложной информационной системы. Идея произведения реализуется художником в процессе организации композиции, которая одновременно, является планом прочтения сюжета зрителем.

Именно, произвольное внимание обеспечивает активизацию мышления, формирование интеллектуального развития, научного прогресса в целом. Находясь в непрерывном функциональном взаимодействии, непроизвольное и произвольное внимание помогают человеку получать и накапливать информацию, логически структурировать и синтезировать на пути к стадии готовой художественной формы – реализму. Необходимо освоение нескольких уровней уточнения информации с тем, чтобы добиться максимально правдивого, без искажений, представления данных. Причем, реалистическое представление данных – наиболее емкое по объему и сложности системного устройства. Именно, поэтому теоретики искусства понимают реализм, как одну из главных особенностей художественного познания. Важность реалистического представления данных несомненна. В одних случаях это – портрет, в котором заказчик хочет узнать свой образ. Или, нам, живущим в XXI веке, интересно выяснить как, например, художник П.А. Федотов критически осмысливал образ жизни своих современников в XIX веке. В других случаях, это – карта, в которой картограф обязан, с определенной точностью, предоставить правдивую информацию потребителю. Писатель наделяет своих персонажей личностными качествами. От точности в работе чертежника и архитектора зависит прочность и качество, а это уже решение вопросов безопасности.

Предлагается следующее определение реализма: Реализм – стадия готовой художественной формы в цикле максимально возможных совершенствований представления данных.

Новое определение не претендует на изменение исторически сложившихся взглядов на развитие реализма, скорее наоборот, направлено на то, чтобы объединить все теоретические вопросы в единое системное знание науки об управлении и связи – кибернетики, где любая информационная единица является сообщением.

Ясинская О.Л.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

МУЗЫКАЛЬНОЕ ТВОРЧЕСТВО НА БАЗЕ DIGITAL AUDIO WORKSTATION ABLETON LIVE (ОСНОВНЫЕ ВОЗМОЖНОСТИ ДЛЯ СИСТЕМЫ СОВРЕМЕННОГО МУЗЫКАЛЬНОГО ОБРАЗОВАНИЯ)

Интенсивное развитие компьютерных технологий привело к обширному использованию их в различных видах музыкального творчества. Это направление находит активное развитие в системе подготовки современного музыканта. Современный музыкально-компьютерный инструментарий позволил разнообразить и обогатить варианты исполняемого музыкантом материала в реальном времени.

Одним из важнейших инструментов современного электронного музыканта является MIDI-контроллер. С его помощью происходит управление виртуальными или аналоговыми синтезаторами, семплерами или эффектами. Также многие модели современных контроллеров позволяют работать даже с опциями программного обеспечения, такими как play, stop,volume, loop, channel и т.д. Возможности Digital Audio Workstation Ableton Live позволяют работать с музыкальным материалом посредством MIDI-контроллера. Секвенсор Ableton live реализует сессионный режим для живых выступлений, где композиция выглядит в виде набора готовых фрагментов. Это даёт возможность импровизировать и создавать композиции «на лету», предварительно создав основу в виртуальной студии. Ableton Live позволяет подключать любые внешние контроллеры, от традиционных MIDI-клавиатур до экзотических инструментов.

Так как Ableton - это многопрофильная программа, она может быть применена не только для звукозаписи, но и для исполнения и творчества в реальном времени. Этот упрощенный и автоматизированный инструментарий дает практически неограниченные возможности работы с музыкальной палитрой, что делает занятие творчеством более доступным и продуктивным для современного музыканта-исполнителя и музыканта-педагога.

В докладе рассматриваются основные возможности творчества музыканта на базе Digital Audio Workstation Ableton Live в системе современного музыкального образования.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ И ЗДРАВООХРАНЕНИИ

Бланк М.А., Бланк О.А., Дюк В.А.
Россия, Санкт-Петербург, Российский научный центр радиологии и хирургических технологий Министерства здравоохранения Российской Федерации, Санкт-Петербургский институт информатики и автоматизации РАН

ОПЫТ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ DATA MINING ДЛЯ ВЫЯВЛЕНИЯ ФАКТОРОВ, ВЛИЯЮЩИХ НА ВЫРАЖЕННОСТЬ ПОСТЛУЧЕВОЙ ГЕМОДЕПРЕССИИ

Выявление причин, определяющих тяжесть гематологических последствий воздействия ионизирующего излучения на организм человека актуально не только для специалистов, занимающихся радиотерапией злокачественных новообразований. Эти сведения необходимы для организации защиты и обеспечения оптимальной помощи населению путём профилактики и прогнозирования последствий техногенных и иных катастроф.

Адекватной моделью лучевой болезни служат гематологические последствия терапевтического лучевого воздействия (так называемого субтотального облучения тела (СТОТ)), успешно применявшегося в конце XX века в лечении онкологических больных, в особенности, в случаях множественной устойчивости опухоли к лекарственным препаратам (MDR-синдром, от «multiplied drug resistance»). Длительные наблюдения показывали, что выраженность и длительность гематологических последствий облучения больших объёмов тела в одинаковых дозах существенно различаются. С целью выявления эндогенных и экзогенных факторов, определяющих такие различия, было предпринято наше исследование.

Данные 74 больных злокачественными лимфомами, получивших в качестве одного из этапов лечения субтотальное облучение тела в суммарной дозе от 1,5 до 6,4 Гр., были проанализированы при помощи методов традиционной математической статистики, составляющих основу прикладных пакетов программ (StatGraphics Plus for Windows v. 5.0.), программы для построения деревьев решений AnswerTree v. 2.1 (SPSS), программы для поиска логических закономерностей методом ограниченного перебора WizWhy (Wizsoft) и специального пакета программ «Система Deep Data Diver™ (DDD)», разработанного В.А.Дюком и М.Г.Асеевым. При составлении компьютерной базы данных, кроме даты, диагноза, пола и возраста пациента, характеристик СТОТ и гемодепрессивного эффекта, учитывались показатели геомагнитной активности во время проведения лучевой терапии.

В результате традиционного статистического анализа были выявлены следующие статистически достоверные взаимосвязи.

1. Зависимость степени тромбоцитопении от возраста пациента во время проведения СТОТ.
2. Зависимость степени тромбоцитопении от уровня относительного снижения количества лейкоцитов (надира лейкоцитов) и степени лейкопении.
3. Зависимость степени тромбоцитопении от минимального уровня суточного значения геомагнитного К-индекса во время проведения лечения.

После проведения традиционных статистических процедур все данные пациентов вновь подвергли обработке при помощи технологий Data Mining.

В первую очередь был использован математический прием построения деревьев решений при помощи системы AnswerTree v. 2.1 (SPSS), базирующейся на процедуре CHAID (chi square automatic interaction detection), основанной на критерии хи-квадрат. Система AnswerTree обнаружила только одно приемлемое по точности и полноте логическое if-then правило: «если степень лейкопении равна 4 и пациент мужского пола, то степень тромбоцитопении равна 4». Правило покрывает 18 объектов и делает 1 ошибку.

Применение системы WizWhy (WizSoft), кроме факторов, выявленных методами традиционного статистического анализа, показало достоверную зависимость глубины лейкопении и пола пациента, разовой и суммарной дозы, геомагнитной обстановки во время облучения и фазы эндогенного многолетнего ритма. Проведение первого курса СТОТ в конвенциональном режиме, в периоды снижения геомагнитной активности, у пациентов, возраст которых (в зависимости от пола) кратен 2 или 3, приводило максимальному снижению количества лейкоцитов. Наиболее чётко эта связь проявилась у женщин.

Логические правила, сформулированные системой Deep Data Diver, повторили закономерности, обнаруженные другими математическими процедурами, расширили отрезок многолетнего эндогенного ритма, неблагоприятный для проведения системной ЛТ и подтвердили устойчивые корреляции степени лейкопении и значения К-индекса.

Обобщение результатов традиционного статистического анализа и данных, полученных при помощи технологии Data Mining, показывает следующее:

1. постлучевые лейкопения и тромбоцитопения взаимосвязаны;
2. понижение геомагнитного фона, так же, как и его резкое повышение усиливают гемодепрессивный эффект ионизирующего излучения;
3. выраженность гемодепрессии зависит не только от возраста пациента, но и от фазы эндогенного многолетнего ритма.

Гайсин В.А., Виноградова Т. В., Кулинкин Б. С., Никонорова М. Л., Тишков А. В., Яицкий А.Н.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова

ПРИМЕНЕНИЕ ПОЛИЛИНГВАЛЬНЫХ ПОСОБИЙ ПРИ ОБУЧЕНИИ ИНОСТРАННЫХ УЧАЩИХСЯ

Концепция экспорта образовательных услуг Российской Федерации на период 2011–2020 гг. определяет принципы, основные цели и задачи Российской Федерации в области предоставления образовательных услуг иностранным гражданам в России и за ее пределами. Экспорт образовательных услуг в настоящее время является одним из приоритетных направлений внешней политики нашей страны, способствующий укреплению внешнеэкономической и политической стабилизации России, популяризации в иностранных государствах российской науки, образования, культуры и русского языка. Особое место в программах подготовки специалистов для зарубежных стран уделяется медицине. За неполные 70 лет международной образовательной деятельности, Первый Санкт-Петербургский государственный медицинский университет им. академика А.П. Павлова обучил медицинским специальностям представителей многих стран Европы, Азии и Америки. В настоящее время в университете учатся студенты более 70 стран мира, в том числе из Бразилии, Ирана, Ирака, Египта, Китая, Сирии, Монголии, Греции, Марокко, Туниса, США, Финляндии и т.д.

Структурным подразделением факультета иностранных студентов университета является подготовительное отделение для иностранных граждан, на котором слушатели обучаются общению на русском языке. Специальная математическая терминология и постановка физических задач на первых месяцах обучения им не понятны. Учитывая, что уровень базового образования в ряде стран значительно ниже, чем в России, перед преподавателями ставится чрезвычайно сложная задача довести уровень компетенций иностранных учащихся до базового уровня компетенций российских студентов – первокурсников. Для решения поставленной задачи на кафедре физики, математики и информатики было создано полилингвальное учебное пособие по физике на четырех языках: русском, английском, китайском и арабском. Выбор арабского и китайского языков обусловлен тем, что в последние годы значительно выросло количество иностранных граждан желающих обучаться в университете среди граждан Китая и ряда стран, в которых преобладает арабский язык.

Полилингвальное пособие включает несколько лабораторных работ, в процессе выполнения которых слушатели формируют и развивают информационно-технологические компетенции, включающие постановку физической задачи, разработку математической модели, при построении которой применяются дифференциальные уравнения первого и второго порядка, проведение эксперимента, математическую обработку результатов измерений и определение погрешностей измерений. Эффективность обучения и коррекция «остаточных» знаний осуществляется с помощью математического диктанта.

Дидактические и наглядные материалы: раздаточные таблицы, плакаты, полилингвальное учебное пособие широко используются при выполнении лабораторных работ. Наиболее существенные результаты были получены при проведении занятий в компьютерных классах кафедры, в которых к традиционным средствам обучения добавляются и виртуальные, такие как прикладной табличный процессор MS Excel, разработанное специализированное программное обеспечение. Использование при проведении лабораторных занятий мультимедийных презентаций также способствуют усвоению больших информационных потоков информации, физической и математической терминологии, усвоению научного стиля речи по предметам медицинская физика, математика, медицинская информатика.

Приобретенные информационно-технологические компетенции позволили развить такие профессиональные компетенции обучающихся, как овладение научно-исследовательской и технологической деятельностью. Развитие личностных качеств слушателей позволило адаптироваться иностранным учащимся к непростому для них дальнейшему обучению в Первом Санкт-Петербургском государственном медицинском университете имени академика И.П. Павлова.

Выпускники подготовительного отделения демонстрируют базовые знания в предметных областях, способность применять знания на практике, приверженность этическим ценностям, понимание культуры и обычаев других стран, навыки межличностных отношений, способность работать в международной среде.

Денисова Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ВЛИЯНИЕ СЛЕЖЕНИЯ В СЕТИ ИНТЕРНЕТ НА ПСИХОФИЗИОЛОГИЧЕСКОЕ БЛАГОПОЛУЧИЕ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ

Согласно данным на 2016 год, 49,2% населения Земли пользуются сетью Интернет. 61,4% людей, проживающих на территории Российской Федерации, являются интернет-пользователями. Возрастающее значение всемирной сети во всех сферах повседневной жизни приводит к дискуссиям о допустимой степени государственного контроля за контентом сайтов и онлайн-активностью пользователей. Актуальность настоящего исследования обусловлена необходимостью всесторонне оценить последствия такого вмешательства, их влияние на общественное благополучие. В качестве предмета исследования выбрано влияние слежения в сети Интернет на психофизиологическое состояние пользователей.

Цель исследования – выявить степень значимости интернет-приватности для психофизиологическогого благополучия интернет-пользователей, а также факторы, влияющие на её положение в потребностной сфере человека.

Для достижения цели необходимо провести анализ источников, содержащих экспериментальные данные, и систематизировать их результаты в рамках теории пирамиды потребностей А. Маслоу.

В докладе рассмотрен ряд теоретических и экспериментальных исследований зарубежных авторов, которыми были сделаны следующие выводы:

1. В сети Интернет проявляется так называемый «эффект паноптикона»: даже если человек не знает, а только подозревает о том, что за ним ведётся наблюдение, его психофизиологическое состояние претерпевает изменения. К ним относятся снижение самооценки и коммуникабельности, повышение уровня ситуативной тревожности и конформности.

2. Можно выделить два стрессора, неразрывно связанных со слежением за активностью интернет-пользователей. Во-первых, сам факт слежения, даже гласного (например, оборудование рабочих мест системами контроля производительности), снижает уровень продуктивности и психологического удовлетворения, получаемого от деятельности, и повышает уровень связанного с ней стресса. Были выявлены такие психофизиологические последствия электронного надзора, как повышенные утомляемость и раздражительность, депрессия, тревожность и соматические недомогания.

Во-вторых, ситуация, когда пользователь сети Интернет не знает, кто именно, когда и с какой целью следит за ним, является ситуацией неопределённости. Неопределённость же, согласно ряду исследований, является более сильным стрессором, чем неизбежное негативное событие.

3. Одним из важных условий психофизиологического благополучия человека является наличие сетей социальной поддержки. Однако в условиях возможного слежения количество и качество межличностных контактов снижается. Потребность в самоцензурировании приводит к неспособности формировать глубокие эмоциональные привязанности и дистанцированию от своего окружения.

4. Наличие реальной или предполагаемой угрозы жизни и благополучию (например, смоделированная кибератака) вызывает изменения в потребностной сфере человека. Приоритетной становится потребность в безопасности, поэтому доверие к институтам власти возрастает, как и поддержка политики контроля за сетью Интернет и её пользователями. К психофизиологическим последствиям кибертерроризма также относятся стресс, тревожность и чувство незащищённости.

Обобщая собранную информацию, можно придти к следующим выводам:

1. Потребность в интернет-приватности относится к средним и высшим уровням пирамиды потребностей Маслоу, так как она непосредственно связана с такими потребностями, как потребность в принятии, потребность в уважении и потребность в самоактуализации. В то же время, потребность в безопасности является базовой по отношению к этим уровням. В случае, если она фрустрирована, потребность в интернет-приватности игнорируется, и возникает социальный запрос на контроль за сетью Интернет.

2. В условиях удовлетворённости базовых потребностей населения слежение в сети Интернет приводит к снижению качества жизни и продуктивности деятельности за счёт психофизиологических последствий стресса.

3. Контроль за онлайн-активностью приводит к атомизации общества, препятствует укреплению горизонтальных связей в нём. На уровне индивида это означает затруднение доступа к эмоциональной поддержке, служащей важным ресурсом стрессоустойчивости и способствующей социальной адаптации.

Таким образом, в сети Интернет, как и вне её, личное пространство является необходимым условием психофизиологического благополучия человека и общества. Это необходимо учитывать при разработке концепций дальнейшего развития Всемирной сети.

Жвалевский О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОД АНАЛИЗА ФРАКТАЛЬНОЙ ДИНАМИКИ И ЕГО ПРИЛОЖЕНИЕ К ОБРАБОТКЕ ТЕНЗОТРЕМОРОГРАММ

При диагностике болезни Паркинсона регистрируется тремор. Треморограммы, регистрируемые при помощи тензорезистивного датчика по методике, предложенной проф. С.П.Романовым , носят название тензотреморограмм (ТТГ). Цель регистрации ТТГ — исследование процессов регуляции движений и выделение признаков, характерных для болезни Паркинсона.

Выделение признаков происходит на основании математического анализа ТТГ (при помощи всевозможных методов обработки временных рядов), вычислении множества вариантов наборов потенциально информативных признаков и применении методов машинного обучения.

По своей сути, речь идёт о создании системы распознавания, позволяющей относить с заранее заданной точностью (в смысле выбранного критерия качества распознавания) поступающие на вход системы распознавания объекты к одному из заранее заданных классов выбранной классификации.

Построение системы распознавания производится в два этапа.

На первом этапе исходные экспериментальные данные (временные ряды) подвергаются обработке различными методами анализа временных рядов, и из всего множества вычисляемых с их помощью характеристик выбираются те характеристики или признаки, которые, потенциально, могут принять участие в построении решающих правил.

На втором этапе, выбираются методы машинного обучения, выбирается критерий качества распознавания, и применяются всевозможные алгоритмы отбора информативных признаков.

Проф. Р.И.Полонниковым был предложен метод анализа фрактальной динамики (АФД).

Этот метод был разработан для анализа электрической активности мозга и предназначен для обработки электроэнцефалограмм (ЭЭГ).

Этот метод содержит в себе элементы спектральных, статистических и фрактальных методов анализа временных рядов.

Представляется целесообразным построить на базе метода АФД методику математической обрабПроф. Р.И.Полонниковым был предложен метод анализа фрактальной динамики (АФД).

Этот метод был разработан для анализа электрической активности мозга и предназначен для обработки электроэнцефалограмм (ЭЭГ).

Этот метод содержит в себе элементы спектральных, статистических и фрактальных методов анализа временных рядов. Алгоритм метода АФД предполагает выполнение трёх этапов:

1. Сегментация временных рядов. Здесь выбирается длина сегмента и исходный (анализируемый) временной ряд разбивается на фрагменты указанной длины. Длина сегмента выбирается исходя из условия квазистационарности временного ряда (сегмента).

2. Вычисление на каждом сегменте определённого набора признаков. В первую очередь, вычисляется спектр. Этот спектр (спектр мощности или, сокр. СПМ) используется не сам по себе (для того чтобы оценить вклад той или иной гармоники), а для того, чтобы построить двупараметрическую модель огибающей СПМ и использовать параметры моделей (полученных на всех сегментах) в качестве первого блока признаков. Во вторую очередь, каждый временной ряд (сегмент) «сворачивается» в матрицу (по методу «Гусеница») и к этой матрице применяется метод главных компонентов (МГК). В результате применения МГК возникает две группы объектов: собственные числа и соответствующие им собственные вектора. Собственные вектора используются для построения главных компонентов временного ряда и для последующего «восстановления» временного ряда и вычисления вариационного размаха восстановленного временного ряда. Собственные числа используются не сами по себе, а в качестве соотношений — чисел обусловленности. Вариационный размах и числа обусловленности составляют второй блок признаков.

3. Вычисление интегральных показателей. Здесь берутся признаки, которые вычисляются на каждом сегменте, и для каждого такого признака вычисляются интегральные показатели.

В работе рассмотрена задача построения системы распознавания, основанная на анализе тензнотреморограмм. В качестве основного источника потенциально информативных признаков предполагается использовать модифицированный метод анализа фрактальной динамики.

Особое внимание в работе уделено структуре ошибок распознавания. Это необходимо для того, чтобы оценить точность и достоверность получаемых результатов, что приобретает особую актуальность в условиях малой выборки.

В то же время, появляется существенно большая гибкость при выборе и настройке моделей (решающих правил), а сами результаты распознавания становятся лучше интерпретируемыми и более надёжными, поскольку в случае более детальной структуры ошибок распознавания, появляется возможность направленной оптимизации критерия.

Игнатьев М.Б., Сурженко Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Институт эволюционной физиологии и биохимии им.Сеченова РАН

МОДЕЛИРОВАНИЕ ОРГАНИЗМА ДЛЯ УМЕНЬШЕНИЯ ВРАЧЕБНЫХ ОШИБОК

Компьютерное моделирование организма является важным средством повышения качества здравоохранения. Для лечащего врача важно рассмотрение организма прежде всего на уровне органов и при построении лингво-комбинаторной модели мы будем исходить из общепринятого набора органов - органы движения (кости, мышцы, связки) », «органы пищеварения», «органы дыхания», «мочеполовые органы», «кроветворная и лимфатическая системы», «центральная нервная система», «периферийная нервная система», «железы внутренней секреции», «кожа и сенсорные системы», лингвистическое уравнение организма будет содержать девять переменных A1*E1 + A2*E2 + . . .+ A9*E9 = 0

а структура эквивалентных уравнений будет иметь вид

E1 = U1*A2 + U2*A3 + U3*A4 + U4*A5 + U5*A6 + U6*A7 + U7*A8 + U8*A9
E2=-U1*A1+U9*A3+U10*A4+U11*A5+U12*A6+U13*A7+ U14*A8+U15*A9
E3=-U2*A1-U9*A2+U16*A4+U17*A5+U18*A6 +U19*A7+ U20*A8+U21*A9
E4 = - U3*A1-U10*A2-U16*A3+U22*A5+U23*A6+U24*A7+U25*A8+U26*A9
E5 = - U4*A1-U11*A2-U17*A3-U22*A4 +U27*A6+U28*A7+U29*A8+U30*A9
E6 = - U5*A1-U12*A2-U18*A3-U23*A4-U27*A5+U31*A7+U32*A8+U33*A9
E7 = - U6*A1-U13*A2-U19*A3-U24*A4-U28*A5-U31*A6+U34*A8+U35*A9
E8 = - U7*A1-U14*A2-U20*A3-U25*A4-U29*A5-U32*A6-U34*A7+U36*A9
E9 = - U8*A1-U15*A2-U21*A3-U26*A4-U30*A5-U33*A6-U35*A7-U36*A8

где U1, U2, . . . ,U36 – произвольные коэффициенты, которые могут быть использованы для настройки модели; A1 – характеристика органов движения, E1 – изменение этой характеристики, и т.д. В модели может использоваться большее количество органов, но тогда она будет менее наглядна. Вопрос выбора главных органов для моделирования решают медики. Следует заметить, что характеристики каждого из органов меняются со временем, от характеристик ребенка через характеристики взрослого человека до характеристик пожилого, таким образом может моделироваться процесс старения. Эта модель используется в страховой медицине. Наличие аналитической модели организма открывает возможность отыскания аттрактора организма – если он функционирует, то имеет место жизнь. Главная цель моделирования организма – уменьшить количество врачебных ошибок. В настоящее время в США погибает каждый год из-за врачебных ошибок свыше 100 тысяч человек, что является юридическим фактом. Эту модель можно использовать при принятии решения по пересадке органов. Успехи современной медицины позволяют пересаживать почки и даже сердце, лишь бы был соответствующий донор. Но при пересадке органов имеется много проблем. Как можно интерпретировать операцию по пересадке органов в рамках нашей модели? Это означает, что скачком меняются характеристики какого – либо органа, Ai . Что при этом происходит с организмом в целом? Организм начинает адаптироваться к изменившимся условиям и появляются две альтернативы. Первая альтернатива – адаптационных возможностей организма оказывается достаточно, чтобы ассимилировать новый орган, который приживается. Вторая альтернатива – адаптационных возможностей организма оказывается недостаточно, новый орган отторгается, организм может погибнуть. Для того, чтобы исследовать эту проблему до операции пересадки и нужна модель организма.

Никонорова М.Л., Юрьева О.А.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова

СПИРОМЕТРИЧЕСКОЕ И БРОНХОЛИТИЧЕСКОЕ ИССЛЕДОВАНИЯ В СРЕДЕ БД ACCESS

Деловая игра является формой воссоздания предметного и социального содержания профессиональной деятельности, моделирования систем отношений, разнообразных условий профессиональной деятельности, характерных для данного вида практики.

В деловой игре каждый участник находит решение своей отдельной задачи в соответствии со своей ролью. Общение в деловой игре воспроизводит общение людей в процессе реальной деятельности. Деловая игра способствует обучению совместной деятельности и сотрудничеству, относится к интерактивным типам занятий.

Вид деловой игры, который будет использован на практике:

1. по типу практики, воссоздаваемой в игре и целям: учебный, с ограничением времени.

Практическая значимость деловой игры – понимание, владение основами ведения и создания базы данных, что необходимо будущим врачам в повседневной жизни и для реализации своих научных интересов.

Цель занятия: формирование новых теоретических знаний по функциональной диагностике легочной патологии; формирование практических умений структурирования большого массива разноплановых данных; закрепление теоретических знаний и сформированных практических умений при самостоятельном проведении спирометрии и занесении результатов исследования в БД; формирования правильного позиционирования врач- пациент, м/с- пациент.

Продолжительность изучения темы: 80–90 минут.

– по оценке деятельности: балльная оценка деятельности студентов;

2. по конечному результату: свободная, открытая игра – заранее известного ответа нет, студенты работают над решением неструктурированной задачи.

Тема занятия: освоение студентами навыков работы с базой данных Microsoft Access на примере базы данных разработанной для ввода данных функциональных легочных тестов.

– по конечной цели: обучающая игра, направлена на появление новых знаний и закрепление навыков участников.

Учебная задача: сформировать конструктивный подход к обработке данных, отработать навыки сотрудничества врач–пациент, м/с–пациент.

Для решения учебной задачи Обучающийся должен знать:

– структуру БД Access–2010;
– физиологию внешнего дыхания.

В результате решения учебной задачи Обучающийся развивает информационно–технологическую компетентность, профессиональную компетентность, которая включает:

– работу со стандартной профессиональной медицинской БД;
– овладение техникой проведения спирометрии;
– информационную расшифровку аббревиатур функциональных легочных тестов.

3. по методологии проведения: имитационная и игровая модель, цель которой создать у студентов представление, как следовало бы действовать в определенных условиях в соответствии с заданием.

Имитационная модель отражает выбранный фрагмент реальной действительности, который можно назвать прототипом модели профессиональной деятельности специалиста в учебном процессе. Игровая модель является фактически описанием работы участников с имитационной моделью, что задает успешность взаимодействия в профессиональной деятельности специалиста.

Межпредметные и внутрипредметные связи отражены в последовательности медицинская информатика – терапия, хирургия.

Оснащение занятия: компьютерный класс, проектор, спирограф, стерильные мунштуки, носовые зажимы, база данных MS Access, методическое пособие по технике проведения спирометрии.

Распределение ролей: из числа студентов, по своему желанию, выделяется малая группа, которая состоит из врача, медицинской сестры и пациента. Пациент – участвует в исследовании;

Медицинская сестра заносит данные о враче и пациенте в БД Пульмонология, оформляет результаты исследования в виде файлов. Врач проводит исследование.

Оценка деятельности студентов – участников игры складывается из анализа выработанного и принятого решения, самооценки, обобщения и рекомендаций, а также реализации деловой игры в установленное нормативами время.

Никонорова М.Л., Юрьева О.А., Тишков А.В.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова

АНАЛИТИЧЕСКАЯ ВИЗУАЛИЗАЦИЯ СТАНДАРТОВ СПИРОМЕТРИИ

Впервые выделена актуальность развития информационных технологий в проекте «Концепция развития системы здравоохранения в Российской Федерации до 2020 г.» в разделах проекта Концепции 2.7 и 4.2.8 «Информатизация здравоохранения». Развитие информационных технологий и современных коммуникаций, появление в клиниках большого количества автоматизированных медицинских приборов и компьютеров привело к значительному росту медицинских информационных систем (МИС). Современная концепция МИС предполагает объединение электронных записей о больных с архивами медицинских изображений и финансовой информацией, данными мониторинга с медицинских приборов, результатами работы автоматизированных лабораторий и следящих систем, наличие современных средств обмена информацией (электронной внутрибольничной почты, Internet, видеоконференций и т.д.).

Таким образом, МИС представляет собой массив данных определенной структуры, в состав которой включены инструменты для систематической организации, понимания и использования этих данных с целью принятия стратегических решений. МИС является хранилищем данных и четыре ключевых понятия выделяют это хранилище данных среди других систем (например, реляционной базы данных, системы обработки транзакций и др.): предметное ориентирование, объединение

(интегрирование), временные рамки и энергозависимость. На базовом уровне медицинская информационная система осуществляет компьютерную поддержку врачей разных специальностей. Она содержит информацию, которая отражает электронные персональные медицинские записи, позволяет вести электронную историю болезни, хранить ее на различных носителях, искать и создавать отчеты в соответствии с информационными запросами. Большая часть медицинских информационных систем использует операционные системы семейства Microsoft Windows. Общее количество МИС, работающих только под управлением СУБД Microsoft, или требующих операционную систему корпорации Microsoft, составляет в России свыше 60%.

На кафедре физики, математики и информатики была создана стандартная база данных «Пульмонологические исследования» в среде MS Access, позволяющая вести учет измерений отношений «поток-объем-время» в процессе выполнения человеком медленных и форсированных дыхательных маневров с полной амплитудой измерения объема. Спирометрия – это метод измерения функционального состояния легких, который используется для качественной и количественной оценки их функционального состояния. Заболевания легких, разные этапы лечебных и диагностических процессов, таких как, выявление нарушений, оценка и обоснование эффективности проводимой терапии, просмотр динамики заболевания, экспертиза трудоспособности и пригодности к работе в определенных условиях, массовые и эпидемиологические исследования групп населения находят свое отражение в том или ином характере замедления форсированного выдоха или спокойного вдоха. Все измеряемые показатели в проводимом исследовании представляются в виде числовых данных.

БД «Пульмонологические исследования» имеет простой интерфейс, содержит общие сведения о пациенте, анамнез жизни, результаты первичного осмотра и объективного обследования. Все внесенные результаты исследования соответствуют системе «должных» (среднестатических) величин показателей спирометрии по Клементу. Удобно и безошибочно вводить данные позволяют столбцы подстановки, помогающие быстро заполнять записи с часто повторяющейся информацией. Так как все физиологические величины являются вариабельными, то каждая величина имеет свой диапазон с разбросом значений показателя при воспроизводимости и повторяемости, что позволяет оценивать их критерием градации с помощью выпадающего списка. БД содержит 16 окон для ввода и анализа данных полученного исследования. В БД имеется возможность создавать отчеты как по одному пациенту и его обследованиям, так и по обследованиям, проведенным в течение месяца для всех пациентов.

Различные аспекты будущей профессиональной деятельности и моделирование различных отношений между врачом и пациентом позволяют отразить образовательные технологии. Практическое занятие позволяет сформировать новые теоретические знания по функциональной диагностике легочной патологии и информационно-технологические компетенции, включающие структурирование больших массивов разноплановых данных, теоретические знания и практические умения при самостоятельном проведении спирометрии, информационную расшифровку аббревиатур функциональных легочных тестов, внесение результатов исследования в стандартную базу данных.

Визуализация данных в БД «Пульмологические исследования», отражающая структуры и закономерности исследуемых показателей, может в дальнейшем являться источником информации для последующего анализа данных и поддержки принятия решений в повседневной практике врача.

Попов А.И.
Россия, г. Архангельск, Северный (Арктический) федеральный университет имени М.В. Ломоносова, Высшая школа информационных технологий и автоматизированных систем, лаборатория информатизации прикладных исследований

О СОСТОЯНИИ ИССЛЕДОВАНИЙ В ОБЛАСТИ ЭЛЕКТРОГАСТРОЭНТЕРОГРАФИИ В СЕВЕРНОМ (АРКТИЧЕСКОМ) ФЕДЕРАЛЬНОМ УНИВЕРСИТЕТЕ НА 2016 ГОД

Электрогастроэнтерография (ЭГЭГ) –- электрофизиологический метод исследования моторики различных отделов желудочно-кишечного тракта (ЖКТ). При периферической ЭГЭГ измерительный сигнал снимается с поверхности тела пациента.

Привлекательность ЭГЭГ обусловлена тем, что данный метод, являясь неинвазивным, дает количественную оценку силы, частоты и ритмичности сокращений ЖКТ. Последний всплеск в развитии ЭГЭГ вызван развитием цифровой обработки сигналов и машинного обучения.

В Северном (Арктическом) федеральном университете (САФУ) с 2006 года проводятся исследования в области создания новых методов и инструментов обработки данных ЭГЭГ. В настоящее время работа сосредоточена в лаборатории информатизации прикладных исследований.

Лаборатория ведет научное сотрудничество с врачами д.м.н. Вавринчуком С.А. и к.м.н. Косенко П.М. из Дальневосточного государственного медицинского университета (г. Хабаровск). В настоящее время в распоряжении коллектива имеется около 1500 ЭГЭГ-сигналов, полученных от пациентов и здоровых добровольцев. Для измерений используется аппаратно-программный комплекс «Гастроскан-ГЭМ» производства НПП «Исток-система» (г. Фрязино).

За последние два года получены следующие основные результаты.

Предложен метод контроля качества измерительных сигналов ЭГЭГ, позволяющий обнаруживать артефакты (кратковременные инородные составляющие в сигналах) за счет анализа высокочастотных компонентов ЭГЭГ-сигналов. Предложен также количественный показатель качества ЭГЭГ-сигналов, на основе которого может быть построен индикатор качества для использования непосредственно во время измерительных сеансов. Показан положительный эффект от использования данного метода при измерении ритмичности сокращений желудка. Метод контроля качества ЭГЭГ-сигналов реализован в программном обеспечении HFArt (свидетельство о государственной регистрации № 2015660209).

Разработан программный генератор тестовых ЭГЭГ-сигналов VPatient (свидетельство о государственной регистрации № 2016617400). Предусмотрены два режима работы программы: режим симуляции и режим записи в файл. В режиме симуляции доступ к потоку данных осуществляется по протоколу TCP. Механизм «публикации-подписки» обеспечивает получение как суммарного сигнала, так и его компонентов. Состав и параметры компонентов описываются в xml-формате. Компонентами сигнала являются гармоники с девиациями частоты и амплитуды, постоянный шум, артефакты. В дальнейшем предполагается использовать VPatient при прототипировании улучшенных средств измерений для ЭГЭГ.

Разработано программное обеспечение DiaSten, предназначенное для установки и уточнения степени компенсации стеноза (свидетельство о государственной регистрации № 2016614008) на основе дискриминантного анализа данных ЭГЭГ. Исходными данными для DiaSten являются значения показателей моторики ЖКТ, получаемые с помощью комплекса «Гастроскан-ГЭМ», а также коэффициенты дискриминантной функции. Возможности DiaSten: ввод данных пациента, ввод значений показателей ПЭГЭГ, классификация обследования, вывод результатов диагностики в числовом и графическом виде, формирование HTML-отчета об обследовании. Список используемых параметров и значения коэффициентов функций классификации считываются программой из CSV-файла. В результате обработки данных новых обследований с достоверными диагнозами коэффициенты могут быть уточнены. Таким образом DiaSten может быть встроен в обучаемую систему диагностики в качестве модуля, задачей которого является, по существу, применение текущих знаний системы к данным конкретного обследования. Перспективной является задача разработки такой системы диагностики.

Поддерживается связь проводимых исследований с образовательным процессом. С регулярностью раз в две недели проводится научный семинар лаборатории информатизации прикладных исследований. Студенты проходят в лаборатории практику, выполняют выпускные квалификационные работы. В 2016 году автором выпущено учебное пособие «Компьютерная обработка электрофизиологических сигналов (на примере гастроэнтерографии)», обеспечивающее практическое знакомство с вопросами компьютерной обработки данных электрофизиологических обследований ЖКТ.

Работа проводится при финансовой поддержке в рамках Государственного задания «Создание вычислительной инфраструктуры для решения наукоемких прикладных задач» (Проект № 3628).

Сухов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СОВРЕМЕННЫЕ СРЕДСТВА ПО КОНТРОЛЮ БЕЗОПАСНОСТИ ЛЕКАРСТВЕННЫХ СРЕДСТВ ОНЛАЙН СИСТЕМА ФАРМАКАНАДЗОР

Сферой внимания фармаканадзора является безопасность пациентов. Основные цели: как можно более раннее выявление неизвестных до этого проблем безопасности лекарственных средств, определение частоты случаев побочных реакций, выявление серьезных нежелательных явлений, определение факторов риска при применении лекарственного средства, контроль соотношения «риск-польза» при использовании лекарственного средства, с целью уменьшения риска для жизни и здоровья пациента при приеме препарата.

Областью науки фармаканадзор стал в 1968 году, когда Всемирной организацией здравоохранения была принята Международная программа мониторинга лекарств (International Drug Monitoring Programme), начало системы фармаканадзора в СССР относятся к 1969 году. Тогда был создан отдел учета, систематизации и экспресс-информации о побочном действии лекарственных средств (ЛС). С 1973 года это Всесоюзный организационно-методический центр по изучению побочных действий лекарственных препаратов. Его функциями были выявление, регистрация, анализ побочных реакций на ЛС, а также информирование медицинских работников о побочных реакциях и методах их профилактики.

С 1 января 2016 года вступают в силу «Правила надлежащей практики фармаканадзора» — по сути, перевод Good Pharmacovigilance Practice, переносящие на территорию не только России, но и остальных стран-участниц ЕАЭС, те же правила, которые уже действуют в Евросоюзе.

В настоящее время активно ведется разработка программного обеспечения для фармаканадзора. Основные задачи, которые ставятся перед разработчиками: создание автоматизированной системы приема и учета случаев нежелательных явлений для их обработки, оценки и дальнейшей подачи в регуляторные органы.

Российские разработчики программного обеспечения не отстают от современных тенденций и предлагают онлайн систему фармаканадзор. Основными возможностями данной системы является заполнение карточки случая, куда вводится основная информация о пациенте, препарате и реакции, которая произошла. Так же предоставляется возможность оценки связи между лекарственным средством и нежелательной реакцией. Помимо этого система предоставляет возможность создания и гибкой настройки отчетов, формирования шаблонов отчетов для подачи в регуляторные органы. Имеется возможность отслеживания сроков отправки отчетов согласно законодательству.

Данная система имеет перспективы на фармацевтическом рынке, так как для компаний, разрабатывающих лекарственные средства, главным приоритетом всегда остается безопасность пациентов. Таким образом, возможность быстрой реакции на возникшие нежелательные явления, позволяет значительно увеличить эффективность, как клинических исследований препаратов, так и контролировать безопасность уже представленных на рынке лекарственных средств.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

Алексеев А.А., Груздев В.Н., Кузнецов А.Ю., Шилин Б.В.
Россия, Санкт-Петербург, Санкт-Петербургский центр экологической безопасности РАН, Университет ИТМО

СРАВНЕНИЕ ВИДЕОСПЕКТРОМЕТРОВ ВИДИМОГО-БЛИЖНЕГО ИНФРАКРАСНОГО ДИАПАЗОНА С РАЗЛИЧНЫМИ ТИПАМИ ПОЛИХРОМАТОРОВ

За рубежом видеоспектрометры авиационного и космического базирования активно разрабатываются с начала 80-х гг. прошлого века и сейчас известно более сорока модификаций только для авианосителей. В нашей стране активный интерес к этим приборам проявился в последние два десятилетия, однако, большинство разрабатываемых в РФ приборов видимого-ближнего ИК диапазона 0.4-1.0 мкм построены по схеме с полихроматором на призме, что даёт переменное спектральное разрешение – от 1.5 нм в фиолетовой части спектра до 10 нм в ближнем ИК диапазоне. С точки зрения конечного потребителя этот недостаток является принципиальным и не компенсируется достоинствами призменных приборов – большей светосилой и сравнительной простотой изготовления. Красный-ближний ИК участок спектра 0.6-1.0 мкм является важнейшим для диагностики и дифференциации растительности по положению и крутизне «красного края» вблизи 700 нм и высоте «ИК-плато» 700-900 нм. Ухудшение детальности спектральных кривых и увеличение «спектральной ширины» монохромных изображений в диапазоне 600-900 нм существенно ограничивает возможности решения прикладных тематических задач. Это подтверждается экспериментальным сравнением в лётных и полевых исследованиях видеоспектрометров СПбУИТМО (на дифракционной решётке с постоянным разрешением по спектру) и ЗАО «Лептон» (на призме). Были проанализированы: 1) Серии монохромных изображений (видеоспектральных аэроснимков) и спектры уходящего излучения различных объектов земной поверхности на этих аэроснимках. Аэросъёмка выполнялась с самолёта Ан-30 одновременно обоими приборами. 2) Серии монохромных изображений и коэффициенты спектральной яркости объектов полевой фоноцелевой тестовой панорамы, полученной одновременно двумя приборами, установленными на вращающейся или движущейся платформе. Сравнение кривых уходящего отражённого излучения в авиационном эксперименте и КСЯ объектов при наземных полевых наблюдениях показало, что спектральные кривые видеоспектрометра СПбУИТМО имеют заметно лучшую детальность в диапазоне 700-900 нм, и он является предпочтительным в тематическом использовании, особенно при изучении стресса растений под воздействием различных неблагоприятных факторов. Из них детально изучалось воздействие тяжёлых металлов.

Алексеев В.В., Орлова Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИЗМЕРЕНИЯ В ЭКОЛОГИИ. ОБЕСПЕЧЕНИЕ ЕДИНСТВА ИЗМЕРЕНИЙ ПРИ ФОРМИРОВАНИИ ОЦЕНОК СОСТОЯНИЯ ПРИРОДНЫХ ОБЪЕКТОВ

В современных информационно-измерительных системах (ИИС) контролирующих состояние природных объектов важной задачей является получение достоверных характеристик. Разнообразие природных объектов определяют сложность контроля и оценки их состояния. Исходной информацией для формирования оценок являются результаты контроля характеристик в различных средах (результаты измерения уровня радиации, концентрации примеси вредных веществ, площади загрязнения и др.).

Для обеспечения метрологической сопоставимости результатов контроля различными средствами измерений, их свойства принято выражать в виде неопределенности, которая представляет собой интервальную оценку. В докладе рассматриваются вопросы получения достоверных оценок состояния природных объектов на основе контрольных измерений физических величин, рассматриваются алгоритмы построения шкал на единой метрологической основе для простых, интегральных и сложных оценок.

Простая оценка - результат измерения представляет собой числовое значение контролируемого параметра в единицах представления физической величины. Степень достоверности (неопределенности) полученного результата зависит от: погрешностей средств измерения, используемого метода измерения, принятой модели процесса (погрешность неадекватности модели). Суммарная погрешность полученной оценки характеризуется

математическим ожиданием (в случае смещенной оценки) и законом распределения случайной составляющей ρ(x*).

Качественные отношения представлены в виде нормированной шкалы с равными отрезками и условными отношениями: 0-1 – нет, 1-2 – значительно ниже нормы (ЗН), 2-3 – ниже нормы (НН), 3-4 – норма (Н), 4-5 – выше нормы (ВН), 5-6 – значительно выше нормы (ЗВ), 6-7 – чрезвычайно выше (ЧВ).

Интегральная оценка имеет несколько подходов объединения простых оценок в интегральный показатель оценки качества или состояния объекта. Все они применяют операцию нормирования для обеспечения возможности объединения результатов контрольных измерений.

Сложная оценка формируется с помощью стандартизованных методик объединения наиболее важных характеристик экосистем или природных объектов. Методики позволяют получить значение показателя качества на основании контрольных измерений. Как правило, шкалы этих оценок носят специфический характер и не нормированы. Это затрудняет применение этих оценок для более сложного анализа, получения интегральных показателей качества.

В докладе рассмотрены примеры алгоритмов построения нормированных шкал для простых, интегральных и сложных оценок природных объектов.

Рассмотренные алгоритмы являются метрологической основой для современных ИИС мониторинга природных объектов. Важнейшим при получении оценок является их достоверность. Поэтому в ИИС основное внимание уделяется алгоритмам получения результатов контроля, вопросам надежности определения оценок объектов, идентификации нештатных, предаварийных и аварийных ситуаций, вопросам получения простых и сложных оценок как основы предупреждения чрезвычайных ситуаций в природных экологических системах.

Афанасьев В.П., Васильченко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПРОВЕДЕНИЯ МОНИТОРИНГА АВТОНОМНОЙ СОЛНЕЧНОЙ ЭЛЕКТРОСТАНЦИИ СПБГЭТУ

Характерной особенностью технической деятельности человека в начале XXI веков является быстрый рост энергопотребления. Потребности человечества в энергии по сравнению с существующим уровнем потребления (~13 ТВт) к середине XXI в более чем удвоятся (~30 ТВт). В настоящее время 85% всех энергоустановок работают на ископаемом органическом топливе, запасы которого в настоящее время достаточно велики.

Прогресс, достигнутый в технологии тонкопленочных солнечных модулей, уже сегодня позволил в ряде регионов мира обеспечить паритет в стоимости электроэнергии. Соотношение стоимости «солнечной» и «сетевой» электроэнергии определяет географию экономически эффективной эксплуатации солнечных электростанций в странах с развитыми электросетями. Решить задачу удешевления экологически чистой «солнечной» электроэнергии можно путём перехода на более дешевые тонкопленочные технологии изготовления солнечных модулей.

В работе показано, что при эксплуатации тонкопленочных солнечных модулей в составе электростанций (ЭС) необходимо проводить мониторинг работы, для проведения необходимо иметь программу, в которую будут включены основные инструменты для обработки, визуализации и анализа собранных данных. В случае, если в состав ЭС входят АКБ, то система мониторинга обязательно должна фиксировать данные о напряжениях АКБ для предотвращения ситуации их глубокого разряда и выхода из строя. Так же необходимо фиксировать данные о токах, поступающих на нагрузку. Для корректного определения реального значения эффективности солнечных модулей необходимо достаточно точные данные поступающего уровня инсоляции, не дающие большой погрешности.

Проведенный теоретический расчет мощности прямого, диффузного и полного солнечного излучения показал:

- необходимость уточнения поправочных коэффициентов $K_{\text{гор}}^{\text{пр}_\text{ч}}$ и $K_{\text{гор}}^{\text{диф}_\text{ч}}$ для каждого месяца для наибольшей сходимости с экспериментальными данными эталонных датчиков, и как следствие повышение точности при расчете ожидаемой энерговыработки
- отличную сходимость (менее 1% для полного и прямого излучения и 4% для диффузного) при сопоставлении с экспериментальными данными эталонных датчиков в условиях безоблачного неба для 11 июля
- хорошую сходимость в условиях реальной облачности для полного и диффузного излучения, которая составила менее 20% для июля месяца
- возможность практического применения рассмотренной методики в разрабатываемой программе.

Был описан процесс разработки программы для проведения мониторинга, который включал в себя подготовку станции к проведению мониторинга, заключавшийся в подключении пиранометра

ФЭП-28, с разработкой для него схемы инструментального усилителя напряжения, организации сбора данных о токах, поступающих на нагрузку и напряжениях АКБ. Процесс написания основного кода программы. Реализацией в пользовательском интерфейсе всех необходимых функций, определенных в требованиях и задачах разрабатываемой программы. Весь перечень необходимых функций реализованный в интерфейсе программы:

- сдвиг графика по оси времени
- умножение данных графика на произвольный коэффициент
- построение графиков на независимых осях ординат
- масштабирование
- автоматический расчет площади под кривой, с учетом границ масштабирования
- оперативное задание коэффициентов, используемых при расчете инсоляции
- построение теоретической кривой мощности солнечного излучения на горизонтальную и наклонную поверхность для прямого, диффузного и полного излучения в отдельности
- наложение графиков друг на друга
- экспорт построенных графических зависимостей в области построения графиков в файл, либо на печать.

Проведенный мониторинг солнечной станции с использованием разработанной программы показал высокую эффективность ее использования. Предложенные методика теоретического расчета мощности солнечного излучения и программа, могут быть использованы для мониторинга солнечных станций, а также для оценки энерговыработки и реальной эффективности солнечных модулей.

Биненко В.И.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН

ЭКОЛОГИЧЕСКИЙ ОТКЛИК НА ИЗМЕНЧИВОСТЬ КЛИМАТА ПРИГРАНИЧНЫХ РЕГИОНОВ ЛЕНИНГРАДСКОЙ ОБЛАСТИ РФ, ЭСТОНИИ И ФИНЛЯНДИИ

Исследовано влияние современных изменений климатических параметров (температура, осадки, ветер, экстремальные характеристики) на природные системы и объекты хозяйственной деятельности на территории Ленинградской области и приграничных регионов Финляндии и Эстонии. Экологический отклик на региональные изменения климата особенно важно учитывать при росте числа мультимодальных транспортных комплексов на Финском заливе и увеличением транспортировки энергоносителей и иных опасных грузов в рассматриваемом регионе Балтийского моря.

В рамках выполненного исследования регионального климата особое внимание обращено на зимние периоды года, как наиболее чувствительные к современному изменению климату, на тренды изменчивости основных климатических параметров с целью выработки возможных мер по обеспечению экологической безопасности промышленно-хозяйственных систем, включая адаптацию транспортных и строительных объектов, сельского хозяйственного производства. Средняя продолжительность климатической зимы за последнее десятилетие уменьшилась на 7-10 дней.

За весь период инструментальных метеонаблюдений среднегодовая температура воздуха в г.Санкт-Петербурге повысилась на 2оС/ на 3,4оС за зимний период и на 0,5оС за летний.. Для сравнения среднегодовая температура воздуха для г. Таллинна составила 5,9 °С, а для г. Хельсинки 5,2 °С.

На территории Ленинградской области и приграничных регионов Финляндии и Эстонии функционируют сети метеорологических наблюдений, но нет должной экологической интеграции трансграничных стран для обеспечения их экологической безопасности.

Привлечение данных альтернативных систем наблюдений и совмещение наземных и аэрокосмических наблюдений атмосферы и подстилающей поверхности позволяет повысить значимость и достоверность оценки климатической изменчивости региона за последние десятилетия.

Бузников А.А.
Россия. Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПОЛЯРИЗАЦИЯ ОТРАЖЕННОГО СОЛНЕЧНОГО ИЗЛУЧЕНИЯ – ИСТОЧНИК ИНФОРМАЦИИ ОБ ЭКРЛОГИЧЕСКОМ СОСТОЯНИИ ПРИРОДНЫХ ОБЪЕКТОВ

В настоящее время открываются широкие возможности использования аэрокосмической техники для экологического мониторинга природной среды и совершенствования сельского хозяйства в связи с возможностью в короткие сроки получить оперативную об изменениях состояния почвенного покрова, состояния посевов и других типов природных образований на больших площадях. Особенно важным является получение сведений о влажности почвы. В сельскохозяйственном производстве около 60% всех работ приходится на два весенних месяца. В этот период важно иметь данные о влажности почвы для правильного определения сроков начала пахоты, внесения удобрений, начало

посева и других агротехнических мероприятий. Контроль влажности почв необходим также для правильного режима орошения земель.

Дистанционная оценка влажности почвы связана с рядом трудностей, обусловленных неоднородностью распределения влаги в почве, ограниченной глубиной определения влажности дистанционным методом, влиянием растительного покрова, вещественного состава почвы, промежуточного слоя атмосферы и других природных факторов. Достоверные результаты могут быть получены только при комплексном учете различных факторов в широком диапазоне электромагнитного спектра излучения. Данная работа посвящена анализу лабораторных исследований поляризационного метода индикации влажности различных почв в видимой области спектра. Эта область спектра характеризуется сравнительно большим количеством энергии, отраженным от подстилающей поверхности, что позволяет использовать узкополосные фильтры для устранения фоновых сигналов, например, излучения отраженного от растительного покрова. При увеличении влажности почвы происходит уменьшение отраженного солнечного излучения и увеличения степени поляризации. Поляризации больше зависит от содержания влаги, чем от типа почвы, ее макроструктуры и наклона визируемой поверхности. Поляризация отраженного излучения не завичит от высоты Солнца и постоянна для одного и того же фазового угла, т.е. угла между падающим лучом и рассеянным (лучом визирования). В докладе приводятся и анализируются результаты исследований влажности различных типов почв и делаются выводы о применимости поляризационного метода с аэрокосмических носителей.

Викторов С.В., Спиридонова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН

«ЭСТЕТИЧЕСКИЙ УЩЕРБ» КАК ЭКОЛОГИЧЕСКИЙ ФАКТОР

В контексте обеспечения экологической безопасности береговая зона морей, озер и рек является особым объектом изучении при рассмотрении ряда проблем прошлого экологического ущерба (ПЭУ). Нами выполнено обследование свыше тридцати потенциальных объектов ПЭУ в береговой зоне Финского залива. Результаты анализов образцов грунта в местах расположения трех потенциальных объектах ПЭУ не дают основания говорить о химическом загрязнении в общепринятом понимании:

Загрязнение определено в соответствии с Конвенцией ООН по морскому праву как «внесение человеком, прямо или косвенно, веществ или энергии в морскую среду, включая устья рек, что приводит или может привести в таким негативным последствиям, как вред живым организмам и морской жизни, здоровью человека, затруднение морской деятельности, включая рыболовство и другие виды легитимного использования моря, ухудшение качества морской воды и природной среды».

По нашему мнению, в отношении ряда объектов ПЭУ речь может идти о другом виде экологического неблагополучия, который можно назвать так:

- Эстетическое загрязнение (?)
- Экологический ущерб, причиненный ландшафту (?)
- Эстетический ущерб (?).

В пользу последнего термина в своем учебном пособии "Экологический мониторинг" высказалась Л.Н. Бельдеева, котрая предлагает условно разделитьущерб, причиненный окружающей среде, на экологический, экономический и эстетический. Под экологическим ущербом обычно понимают фактические или возможные потери общества, возникающие в результате негативных изменений среды вследствие антропогенного воздействия. При этом социальные экологические ущербы включают в себя: 1) увеличение смертности и патологических изменений в организме человека;

2) психологический ущерб вследствие неудовлетворенности населения качеством среды обитания; 3) эстетический ущерб от деградации ландшафтов. Надежная экономическая оценка этих эффектов весьма затруднительна, если вообще возможна.

В контексте проблемы «эстетического ущерба» в докладе рассмотрено состояние объекта «Бывшая база заправки подводных лодок» на южном берегу Фиского залива.

Приведены иллюстрации – исторические и современные спутниковые и наземные изображения этого объекта ПЭУ. Содержится информация о взаимодействии авторов с государственными природоохранными органами, которые фактически признали в этом случае наличие «эстетического ущерба».

Относительно береговой зоны Финского залива можно утверждать, что выявленные объекты накопленного экологического ущерба наносят в большой степени именно эстетический экологический ущерб.

Викторов С.В., Спиридонова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН

ОБЪЕКТ «ПРОШЛОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА» В ЦЕНТРЕ САНКТ-ПЕТЕРБУРГА

В 2012 году в Петроградском районе Санкт-Петербурга, на правом берегу реки Малая Нева был сформирован объект прошлого экологического ущерба (ПЭУ) на месте, где с 1919 года располагался ГИПХ - Федеральное Государственное Унитарное Предприятие «Российский научный центр „Прикладная химия“» (ФГУП РНЦ «Прикладная химия», ранее ГИПХ). «В петербургской прессе всё первое десятилетие нового века с разной интенсивностью обсуждался проект новой застройки территории бывшего Ватного острова, то есть фактически территории ГИПХа. Говорилось о необходимости вывода опасного химического учреждения из исторического центра города по соседству с жилыми домами и развития данного участка....Проект новой застройки на данном участке получил название «Набережная Европы», и обращенный к Васильевскому острову плакат с этими двумя словами и логотипом кредитора — банка VTB висел на ограждении со стороны института берега Малой Невы, прохода и проезда по которому не было в связи с закрытым статусом института. К плюсам проекта относят дезактивацию зараженной химикатами территории и обеспечение сквозного движения по набережной с открытием красивых видов на историческую застройку Васильевского острова и художественным оформлением застройки самой набережной, большая часть территории которой с реки выглядела задворками производства. Весной и в первой половине лета 2012 года территория ГИПХ на Петроградской стороне Петербурга вдоль проспекта Добролюбова от Биржевого моста до продолжения переулка Талалихина к берегу Малой Невы расчищена от институтских зданий. Под снос попали и большое здание во всю длину участка 1960-х или 70-х годов постройки, не представлявшее исторической ценности, но бывшее в хорошем состоянии, и краснокирпичные здания здания казенного винокуренного завода ближе к набережной, прежде охранявшиеся государством как памятники промышленной архитектуры. В 2013 году проект «Набережная Европы» был отменён.....»

В настоящее время на территории бывшего ГИПХ сформирован террикон из извлеченного грунта и два карьера. Существует проблема удаления и размещения большого объема зараженного грунта. Проблема обсуждалась в течение нескольких лет, но до сих пор решения нет. Итак, в центральной части мегаполиса («культурной столицы» России) уже 4 года находится объект ПЭУ в составе террикона и двух карьеров - прудов. Координаты центра террикона – 59 град 56 мин 54.05 сек С, 30 град 17 мин 59.84 сек В. По спутниковому изображению определены параметры объекта: высота террикона от 8 до 10 м, длина около 250 м, ширина около 100 м. Длина большего карьера (вдоль реки), заполненного водой, около 260 м, ширина наибольшая – 140 м. Террикон и больший пруд расположены в 20 м от берега реки и являются объектом ПЭУ в береговой зоне реки, впадвющей в Невскую Губу Финского залива. Наличие объекта в центре Санкт-Петербурга и непринятие каких-либо видимых мер по его ликвидации в течение четырех лет демонстрирует реальную ситуацию в области ликвидации ПЭУ в РФ и неспособность исполнительной власти региона решить эти проблемы. Доклад иллюстрирован многочисленными спутниковыми и наземными изображениями.

Воробьев Е.Н., Туленков Н.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ИСПОЛЬЗОВАНИЕ ПАССИВНОГО КОГЕРЕНТНОГО ЛОКАЦИОННОГО КОМПЛЕКСА В ОРНИТОЛОГИИ

Наблюдение за перелетами птиц является одной из основных задач ученых-орнитологов. Периоды миграции обычно связаны с сезонными явлениями, однако не редко оказывают влияние и изменения экологических или кормовых условий на территории обитания птиц. В периоды миграции птиц в воздушном пространстве может возникать сложная орнитологическая обстановка. Традиционные методы визуального и акустического наблюдения не позволяют получить оперативную информацию о местах скопления, высотах, направлениях и скоростях движения птиц.

Мониторинг орнитологической обстановки является актуальной задачей также при обеспечении безопасности полетов гражданской и военной авиации. Столкновения воздушных судов с птицами зачастую приводят не только к повреждениям и, как следствие, дорогостоящему ремонту самолетов, но и авиакатастрофам, влекущими за собой гибель птиц и людей. Предотвращение подобных столкновений требует решения задачи контроля передвижения птиц вблизи аэропортов и на маршрутах следования воздушных судов. Круглосуточный, всепогодный оперативный контроль передвижения птиц не только вблизи, но и на значительном расстоянии от аэропортов и воздушных трасс позволяют обеспечить современные методы радиолокационного мониторинга.

В Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» был разработан пассивный когерентный локационный комплекс (ПКЛ), использующий сигналы цифрового

эфирного телевидения стандарта DVB-T2 в качестве сигнала подсвета целей. В докладе приводятся результаты обнаружения и сопровождения полетов птиц, полученные в ходе экспериментальных исследований разработанного ПКЛ.

Горохов В.Л., Бузников А.А., Витковский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Университет ИТМО

ОБЪЕКТИВАЦИЯ КОГНИТИВНЫХ ОБРАЗОВ И ИХ ВНЕДРЕНИЕ В СРЕДУ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ ДЛЯ ЭКОЛОГИЧЕСКОГО И ТЕХНОСФЕРНОГО МОНИТОРИНГА

В настоящее время результаты экологического и техносферного мониторинга представляют собой терабайтные многомерные массивы (BIG DATA). Выявление фактов аномального поведения объектов мониторинга, представленных такого рода массивами данных, представляет серьезную проблему (проблема BIG DATA).

Одним из путей решения этой проблемы является представление эти данных в виде когнитивного образа возникающего в сознании человека – оператора при динамическом проецировании многомерных данных на экран компьютера. Феномен появления когнитивного образа возникает в сознании человека-оператора при наблюдении оператором динамической проекции данных проецировании многомерных данных на плоскость экрана компьютера. Этот феномен позволяет выявлять особенности в многомерных терабайтных данных вызванные аномальным поведением объектов мониторинга. Однако этот эффект активизации интуитивного сознания можно значительно усилить, если поместить когнитивный образ в виртуальную среду, которая уже сейчас активно формируются программными средствами типа «дополненная реальность».

Для этого для этого требуются алгоритмы и средства объективации когнитивных образов. В данной работе в качестве алгоритма объективации когнитивного образа выбран алгоритм построения 3D изображения по его проекциям. В качестве проекций используются проекции из многомерного пространства данных. Затем полученное 3D изображение, представляющее объективированный когнитивный образ, встраивается в виртуальную среду, позволяющую усилить когнитивный эффект за счет комфортной для человека манипуляцией когнитивным образом. Например: делать томографические срезы и 3D объемное фрагментирование интересных участков когнитивного образа. Все это стимулирует профессиональную интуицию человека и позволяет принимать практически важные решения, поскольку эти решения опираются на объективные многомерные данные мониторинга.

Предлагаемый подход иллюстрируется примерами из области гидрологического и медико-экологического мониторинга.

Горохов В.Л., Маяков А.Н., Бузников А.А., Витковский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Университет ИТМО

НЕПАРАМЕТРИЧЕСКОЕ ОЦЕНИВАНИЕ АНОМАЛИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДАХ И ИХ КОГНИТИВНАЯ ИНТЕГРАЦИЯ

Целью данной работы является предложение и исследование алгоритмов выявления сигналов неизвестной формы в многомерных временных рядах с последующим представлением отдельных временных рядов от каждого объекта (скважины) как точек в многомерном пространстве параметров этих скважин. С помощью средств когнитивной машинной графики эти скважины образуют когнитивные образы, при наблюдении которых видно, как аномальное поведение параметров заданных скважин может быть выявлено в случае многомерных терабайтных массивов.

В настоящее время концепция и технологии когнитивной компьютерной графики получили широкое распространение. В рамках данного направления особую популярность получили методы, основанные на алгоритмах динамического проецирования многомерных данных. Основой этих методов является табличная структура, в которой терабайтные совокупности объектов описываются множеством параметров, образующих в многомерном пространстве «облака точек» представляющих эти объекты, геометрия которых описывает особенности этой совокупности этих объектов. Когнитивная суть методов динамического проецирования состоит в том что, динамическое проецирование (специальными алгоритмами) этих облаков на выделенную плоскость параметров создает изображение движущихся точек, которые психологически, воспринимается сознанием пользователя как псевдо трехмерный образ множества объектов. Замечательным является то, что этот образ отражает особенности структуры многомерного облака данных, что имеет большое практическое значение. Например, в задачах управления в условиях неопределенности.

В данной работе эти технологии распространяются на ситуацию, когда в качестве совокупности объектов выступают состояния объекта в разные моменты времени. Эти состояния количественно описываются множеством параметров. Эта ситуация описывается в многомерном статистическом анализе как модель многомерных временных рядов. Именно для этой модели предлагается

использовать технологию когнитивного динамического проецирования для оперативного выявления особенностей многомерных временных рядов. Визуально наблюдая эти многомерные временные ряды, появляется возможность выявлять на фоне шумов аномальное поведение этих временных последовательностей (резкие всплески, тренды, корреляции и т.д.), которые можно представлять стохастических сигналов. Для количественной объективации обнаруженных аномалий можно использовать достаточно развитые методы теории обнаружения и оценивания сигналов. В рамках этой теории разработаны методы синтеза устойчивых (робастных) алгоритмов обнаружения и оценивания величины подобных сигналов. В данной работе разрабатываются алгоритмы обнаружения и оценивания сигналов, которые моделируют отмеченные выше аномалии (сигналы). Обнаружение осуществляется по каждому временному ряду для каждого параметра. Когнитивные методы визуализации позволяют оперативно выбирать необходимые участки временных рядов, в которых наблюдаются возможные аномалии. Кроме этого в данной работе предлагается полученные оценки величины аномалий по отдельным параметрам для каждого объекта рассматривать как самостоятельные параметры, характеризующие наличие и величину аномалий во временных рядах. Это позволяет для множества объектов, используя когнитивную машинную графику получить когнитивный многомерный образ множества объектов, который визуализирует и выявляет те объекты, в которых наблюдаются аномалии. Полученные результаты иллюстрируются практическим приложением для задач гидрологии (для многомерного мониторинга скважин).

Предлагаемый эргономический подход позволяет визуально заметить многомерно связанные аномалии в терабайтных массивах данных, открывает новые возможности для мониторинга больших природных и техносферных систем. Современные системы статистического анализа SPSS Statistics дополняют и обеспечивают детальный объективный количественные анализ обнаруженных с помощью когнитивных средств техносферных и природных аномалий.

Горяинов В.С., Черноок В.И., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), АО «Гипрорыбфлот»

ИДЕНТИФИКАЦИЯ ГИДРОБИОНТОВ ПО ДАННЫМ ЛИДАРНОГО ЗОНДИРОВАНИЯ

Оптические локаторы (лидары) широко используются для исследования водной среды, начиная с 1970-х гг. Несмотря на разнообразие конструктивных реализаций, в основе данной методики лежит общий принцип: в направлении исследуемого объекта испускается короткий импульс лазерного излучения, а затем фотоприёмник регистрирует излучение, рассеянное в обратном направлении (эхо-сигнал). В качестве информативных параметров эхо-сигнала могут использоваться его временная форма (длительность и интенсивность), а также спектральный и поляризационный состав.

По мере усовершенствования элементной базы и развития методов обработки данных зондирования расширялась сфера применения лидаров в океанологических исследованиях и экологическом мониторинге Мирового Океана. В настоящее время лидарные системы успешно используются для определения мутности воды, концентрации и видового состава фитопланктона, батиметрических измерений, обнаружения рыбных косяков и оценки биомассы в них, а также для поиска различных видов загрязнений, включая нефтяные.

Авторы доклада описывают опыт применения лидаров для дистанционной локации гидробионтов, в том числе личный, полученный в ходе исследований в Белом, Баренцевом, Норвежском, Охотском и Чёрном море. Исследования проводились на базе самолётов-лабораторий Ил-18, Ан-26 «Арктика», L-410 «Норд», Ан-38 «Восток». В докладе приводятся примеры эхо-сигналов от слоёв фитопланктона, различных видов рыб (скумбрия, мойва, сельдь, лосось), медуз, китов и дельфинов. Кроме того, сделаны выводы о временных и поляризационных характеристиках эхо-сигнала, позволяющих отличать гидробионтов от других объектов зондирования, а также определять их видовую принадлежность.

Гринь С.С., Кустов Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

РАЗРАБОТКА АППАРАТНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОГО КОМПЛЕКСА КОНТРОЛЯ БИОТЕСТОВЫХ РЕАКЦИЙ

В настоящее время резко возросла угроза антропогенного загрязнения окружающей среды.

Биотестирование наряду с аналитическими физико-химическими методами является важным инструментом для выявления токсичности различных сред: питьевой, сточной и технологической воды, отходов, вытяжек почвы. В качестве чувствительного к токсичным факторам биообъекта широкое распространение получили инфузории. Имеется ряд тест-реакций для контроля токсичности водных сред с применением инфузорий, среди которых можно выделить: летальность (смертность), хемотаксис (уход из опасной зоны), гальванотаксис (перемещение под действием электрического тока жизнеспособных клеток).

Для контроля биотестовых реакций широкое распространение получил оптический фотометрический метод. Одним из наиболее пригодных фотоприемников для создания биотестовой аппаратуры, способной контролировать распределение микроорганизмов по высоте кюветы, являются линейные фоточувствительные ПЗС элементы (далее ПЗС-линейка). Основной особенностью применения ПЗС-линеек в биотестировании является соизмеримость фоточувствительных элементов с размерами тест-объектов. Для фокусирвоки светового потока, прошедшего через исследуемый раствор, на плоскость фоточувствительных пикселей ПЗС-линейки используется цилиндрическая линза.

Физической основой определения распределенной по кювете концентрации тест-объектов является измерение отношения мощности светового потока в чистой воде и в воде с клетками.

В ходе исследований была разработана математическая модель расчета мощности светового потока, сфокусированного цилиндрической линзой на плоскость ПЗС-линейки. В данной модели учитывается ширина излучающей поверхности светового источник, входная площадь кюветы, а так же ширина пикселей ПЗС-линейки. Зная данные параметры, можно разработать программный алгоритм определения мощности светового потока в чистой воде и в воде с микроорганизмами, и как следствие, получить значение распределенной концентрации организмов по кювете.

Доронин А.П., Петроченко В.М., Козлова Н.А., Шмалько С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОЧИЩЕНИЕ ВОЗДУШНЫХ БАССЕЙНОВ КРУПНЫХ ГОРОДОВ ОТ ЗАГРЯЗНЯЮЩИХ ПРИМЕСЕЙ ПУТЕМ ИНТЕНСИФИЦИРОВАНИЯ ОСАДКОВ

Наличие в крупных городах экологических проблем, связанных с загрязнением их воздушных бассейнов, обуславливает необходимость поиска и разработки эффективности методов и средств, позволяющих существенно снизить концентрацию загрязняющих веществ в атмосферном воздухе. В качестве таковых в настоящей работе предлагается использовать методы и средства очищения воздушных бассейнов крупных городов, основанные на применении средств модифицирования облаков.

Для улучщение экологической обстановки предлагается использовать метод очищения воздушных бассейнов крупных городов от загрязняющих примесей путем интенсифицирования естественных осадков из переохлажденных внутримассовых слоистообразных облаков.

Основным исходным материалом для выполнения настоящей работы явились протоколы сетевого самолетного зондирования (СЗА) ТАЭ-7,7м над Москвой (1953-1964 гг.). Всего проанализировано около 6 тысяч подъемов самолетов-зондировщиков.

Пригодными к интенсифицированию искусственных осадков считались капельные или смешанные облака, дающие осадки, имеющие капельное или смешанное фазовое строение, температуру на верхней границе облаков не выше минус 4□С, вертикальную протяженность облачного слоя не менее 250 м. [1].

Анализ полученных данных показывает, что наиболее благоприятные условия для модифицирования переохлажденных слоистых, слоисто-кучевых облаков с целью интенсифицирования естественных осадков условия для центрального района России наблюдаются в месяцы холодного полугодия (43,8%) с максимумом повторяемости, приходящимся на март. Зимой оценки пригодности облаков к интенсифицированию осадков самые высокие – 45,8%. В летний период в связи с повышением температуры воздуха пригодные к интенсифицированию осадков St – Sc облаков практически не наблюдаются. В переходные сезоны оценка пригодности облаков к модифицированию с такой целью составляют 42,5% весной и 25,9% - осенью.

Приведенные оценки пригодности переохлажденных слоистых, слоисто-кучевых облаков к интенсифицированию осадков по сезонам вполне закономерно объясняются сезонным ходом распределения температуры воздуха в рассматриваемом районе.

Полученные в работе данные имеют практическую ценность, поскольку позволяют, не проводя непосредственно экспериментальные работы, оценить ресурсность облаков в конкретном физико-географическом районе с целью интенсифицирования осадков.

Дюфур М.С. Игнатьев М.Б., Катермина Т.С., Ненашев В.А.
Россия, *Санкт-Петербургский государственный университет, Санкт-Петербургский государственный университет аэрокосмического приборостроения,
г. Нижневартовск Нижневартовский государственный университет

ПРОБЛЕМА ПРОГНОЗИРОВАНИЯ ЛИТОСФЕРНОЙ ПОГОДЫ

Безопасность жизнедеятельности связана с предсказанием землетрясений, от которых погибают каждый год тысячи людей. Для предсказания землетрясений необходимо прогнозировать литосферную погоду по аналогии с прогнозированием атмосферной погоды. В докладе рассматривается вопрос о моделировании движения литосферных плит и террейнов с учетом их масс

по поверхности планеты на основе радионавигационных измерений координат реперных точек литосферных плит. Рассматриваются три уровня прогнозирования – глобальный в масштабе всей планеты, региональный в масштабе отдельной плиты и локальный с учетом сдвигов и разломов на примере Памиро-Тибетского пояса , Сахалина и Скандинавского региона. Наблюдаемый подъем геологических образований Скандинавского региона может иметь существенное влияние на геологическую безопасность Северо-Западного региона России.

Елизаров В.В., Конопелько Л.А., Гришканич А.С., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Всероссийский научно-исследовательский институт метрологии имени Д.И.Менделеева

КАЛИБРОВКА РАМАНОВСКОГО ЛИДАРА С УЛЬТРАСПЕКТРАЛЬНЫМ РАЗРЕШЕНИЕМ

Внедрение в геоэкологический мониторинг рамановского метода получило в последнюю декаду масштабный размах благодаря повышению чувствительности, спектрального разрешения и частотной селекции при детектировании и распознавании химических веществ и соединений в многокомпонентных средах. При этом прогресс в технологии матричных ПЗС фотоприемников позволяет одновременно регистрировать сотни спектральных интервалов, существенно увеличить светосилу входного оптического тракта, сократить массу и габариты лидарного комплекса в целом.

Механизмы формирования предельно высокой чувствительности рамановского лидара можно разделить на две основные группы. Одна – селективность – базируется на синхронном детектировании широкой гаммы химических веществ и соединений, на высоком спектральном разрешении и знании (банке) стоксовых сдвигов для изотопических модификаций массива молекул. Другая – помехозащищенность приемного канала и связанное с ней соотношение «сигнал/шум» – определяется

- выбором рабочего диапазона длин волн, соответствующего экранированию УФ излучения Солнца озоновым слоем в атмосфере,
- регистрацией эхо-сигналов на антистоксовых частотах,
- когерентным усилением антистоксового рассеяния,
- выбором режимов счета фотонов и стробирования,
- гигагерцовой полосой частот детектирования сигналов,
- программой обработки.

В данной работе обоснованы и экспериментально исследованы методы контроля точности указанных спектральных и энергетических характеристик высокочувствительного ультраспектрального рамановского лидара, в особенности, с точки зрения достоверности результатов мониторинга, что остается весьма актуальной проблемой. В докладе приводятся функциональная схема КАРС лидара с разрешающей способностью $\Delta\nu$=0.6 см-1 и селективностью $\nu/\Delta\nu$ >10000, предназначенного для дистанционного обнаружения и спектроскопической идентификации изотопических модификаций молекул при концентрациях до 1 pptv, и пример калибровки приемного канала в широком спектре дискретных длин волн и динамическом диапазоне интенсивностей эхо-сигналов до 10^{12}.

Захаров И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ВЫЯВЛЕННЫЕ СВОЙСТВА ТЕСТ-ОБЪЕКТОВ, ИСПОЛЬЗУЕМЫХ В АППАРАТУРНОМ МИКРОБИОТЕСТИРОВАНИИ

Аппаратурное микробиотестирование, развиваемое автором как направление, основанное на оптических и динамических свойствах организмов малых размеров и требующих малых объемов проб, используется для контроля токсичности водных сред, что является важным региональным фактором сохранения качества воды.

Тест-объекты – организмы, полученные в результате культивации, которая вносит оптические помехи, поэтому требуется процесс очистки как от других видов организмов, так и от частиц корма.

В качестве тест-объектов рассмотрены взвеси инфузорий, сжатые электрическим полем слои инфузорий (перемещающихся как при двукратном, так и многократном изменении полярности поля), а также движущиеся бактериальные слои.

Исследованы оптические свойства биологических тест-объектов и показаны их различия с взвесями частиц и использованы данные отличия для обнаружения и измерения концентраций тест-объектов или их популяционных реакций.

В качестве оптических свойств исследовались спектрофотометрические измерения оптической плотности взвесей инфузорий и бактерий – рассеянных и сжатых физическими полями.

Исследованы динамические характеристики движения биологических объектов, движение которых не сводится к классическим моделям перемещения частиц (броуновского движения,

диффузии). Эти отличия позволяют обнаруживать частиц при мутности и цветности водной среды. Исследуются оптические свойства помех, возникающих в результате остатков корма и возможности их минимизации.

Необходимость неразрушающего контроля движения популяций тест-объектов, как процесса обусловила к использованию, как к универсальным, так и к специализированным средствам.

При создании аппаратурных средств неразрушающего контроля основной идеологией была принята биосенсорная, когда основная функция выполняется биохимическим преобразователем, а вспомогательная функция – средствами измерения биологической реакции.

Результатом развития направления стали разработки аппаратурных средств для микробиотестов, экспресс-микробиотестов, микробиотестов – доза-эффект, позволяющих отразить воздействия на звенья пищевой цепи.

Казанцева А.Г., Завгородний А.В., Величко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДОВ БИОТЕСТИРОВАНИЯ

В 2016 году вступили в силу новые критерии отнесения отходов к I-V классам опасности по степени негативного воздействия на окружающую среду (Приказ Министерства природных ресурсов и экологии РФ от 4 декабря 2014 г. N 536). В сравнении с критериями, действующими с 2001 года, новые критерии при выборе способа определения класса опасности отдают предпочтение экспериментальному методу, а именно биотестированию.

Этот документ наглядно показывает, что области применения биотестирования значительно расширяются. Однако, ограниченность методов, а так же их трудоемкость значительно ограничивает их применимость. Так, по данным Федерального центра анализа и оценки техногенного воздействия, в базе токсикологических методов анализа присутствует всего 24 методики.

В то же время требования к методам контроля качества окружающей среды постоянно ужесточаются. Так, с 2018 года для крупных предприятий вводят обязательный контроль выбросов непосредственно на источниках выбросов загрязняющих веществ в атмосферный воздух. Такие системы предполагают контроль выбросов в реальном режиме времени, что упрощает государственный надзор в области охраны окружающей среды.

Подобное применение методов биотестирования ограничивается отсутствием аппаратурных методов. Из 24 методик только 4 имеют аппаратурное обеспечение.

Большинство методик основано на подсчете количества выживших клеток, помещенных в исследуемую и культивационную среду, а так же подсчет количества рожденных особей. По полученным данным строят кривую EC50. Такое представление результатов позволяет соотносить данные экспериментов с результатами тестов, проводимых на теплокровных, которые были широко распространены в токсикологии.

Значительно меньше методов, основанных на измерении изменения двигательной активности тест-организмов. Следует отметить всего 2 таких теста. Первый заключается в измерении хемотаксической реакции инфузорий P.caudatum при помощи прибора «Биотестер». Второй – в визуальном контроле двигательной активности половых клеток крупного рогатого скота.

Указанные тесты существенно снижают время получения результатов с 48 – 96 часов до 1 часа. Кроме того, использование в качестве тест-объекта половых клеток крупного рогатого скота позволяет избежать процедуры поддержания тест-организмов в рабочем состоянии в тот период, когда экспериментальная работа не проводится, поскольку клетки хранятся в замороженном состоянии. Именно благодаря удобству использования тест-объекта этот метод получил широкое распространение.

Тем не менее, в ближайшем будущем к методам контроля будут применяться несколько другие требования, а именно: автоматизированный контроль параметров тест-реакций. В настоящее время Министерство природных ресурсов активно вводит формы электронного документооборота. Примером таких сервисов являются модули природопользователя, позволяющие подавать предприятиям в электронном виде отчетность в области охраны окружающей среды. После 2018 года планируется введение серверов, позволяющих отслеживать показания систем контроля выбросов предприятий.

Подобные изменения затронут и методы контроля токсичности. Таким образом, методы биотестирования, имеющие современное аппаратурное обеспечение, получат преимущество в применении при контроле токсичности промышленных сбросов.

Каткова И.В., Павлова С.М.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

В настоящее время чрезвычайно важными и актуальными становятся проблемы информационных технологий связанные с экологической безопасностью. Концепция экологической безопасности, сформулированная Н.Ф. Реймерсом, связывает допустимые темпы преобразования окружающей среды со способностью человека адаптироваться к новым экологическим факторам. Поэтому, сохранение и нормальное функционирование нашей планеты первую очередь определяется иерархией сложнейших информационных связей. В значительной степени идет попытка осмысления реалий информатизации общества и нового научного направления – информационной экологии.

В мире в целом необходимо в первую очередь стимулировать работы по своевременной компенсации пагубного влияния негативных тенденций информатизации на здоровье человека и формирующиеся черты молодого поколения. Кроме того, научное направление развития информационного общества поможет определить приоритеты в инвестиционной политике, в модернизации образования и других сферах.

Хотелось бы отметить, что ажиотаж возникший в последние десятилетия вокруг экологических проблем, стимулирует четкое решение и поиск новых путей решения многочисленных проблем, обусловленных развитием информационных технологий и расширением производства компьютеров, поэтому комплекс проблем, возникающий на стыке этических принципов ответственного отношения к природе, заботе о будущих поколениях, сегодня является несомненной необходимостью широкого применения компьютерных технологий в различных областях человеческой деятельности, и в частности в охране окружающей среды.

Разработка концепций ноосферной экологии, связана с генетической безопасностью населения, особенно актуальна в условиях кардинальной перестройки общества с информационной экологической безопасностью. Сейчас задача состоит прежде всего в том, чтобы выработать новую комплексную интегрированную систему охраны биосферы и уже на ее основе осуществлять более разумный дифференцированный подход к вопросом решения информационных технологий в экологии. Фундаментальные процессы обеспечивающие природное равновесие связаны с определенными потоками вещества и энергии через все уровни биосферы. Конечно, ноосферная идея и биосфера имеют характеристику, направленную на консолидацию и усложнение. Для построения информационного общества необходимы кардинальные изменения в культуре, чтобы посредством информационного образования изменить сознание и мировоззрение людей. Победа разума – это единственный выход для человечества.

Развитие информационного общества. Усложнение его инфраструктуры требует тщательного и продуманного управления ресурсами, овладения новыми средствами и методами обработки информации. Наиболее значимыми областями являются геоинформационные системы, системы подготовки и обработки анализа данных, моделирование природных и техногенных процессов. Геоинформационные системы активно используются для решения научных и практических задач: включая экологический мониторинг, обеспечение безопасности человека и т.д. Поэтому взрыв интереса к геоинформационным системам, стремительность их внедрения, различная сфера применения, стратегическое значение геоинформатики дают ей право претендовать на место одной из наиболее перспективных информационных технологий.

В настоящее время исследуются проблемы, связанные с сущностью экологической информации, анализируется метод моделирования, как один из информационных методов обеспечения управления охраной окружающей среды экологический мониторинг. Дается оценка геоинформационных технологий как одного из основных средств обработки экологической информации и формирования единого экологического информационного пространства. Неотъемлемым атрибутом современного технологического производства является требование контроля за влиянием на окружающую среду, социальной и экологической ответственностью предприятий.

Сегодня сложилась качественно иная ситуация: накопленных знаний в целом столько, что их невозможно освоить не только отдельному человеку, но и научному сообществу. Вместе с тем информационные технологии в экологии делают каждый фрагмент знания общедоступным. Изменения задачи, стоящей перед институтом повлечет за собой новые и качественные изменения информационных технологий и методов ориентации в информационном пространстве.

Летучий Ю.А., Новиков А.В., Тимощук А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

МЕТОДИЧЕСКИЙ ПОДХОД К ОБРАЩЕНИЮ С ИСТОРИЧЕСКИМИ ЗАГРЯЗНЕНИЯМИ В АРКТИКЕ

В настоящее время актуальной проблемой Арктического региона является его очистка от исторических загрязнений, значительная часть из которых располагаются на территориях, принадлежащих (ранее принадлежащих) МО РФ. Нанесенный в прошлом экологический ущерб не регулируется в РФ нормативно-правовыми, организационными и финансовыми актами, а правопреемственная практика приводит к определенному конфликту интересов. Если опираться на природоохранное законодательство РФ и оценивать территории с историческими загрязнениями с точки зрения вывода из эксплуатации неиспользуемых сооружений и иных антропогенных объектов, то необходимо руководствоваться статьей 39 №7-ФЗ от 10.01.2002 г: «при выводе из эксплуатации зданий, строений, сооружений и иных объектов должны быть разработаны и реализованы мероприятия по восстановлению природной среды, в том числе воспроизводству компонентов природной среды, в целях обеспечения благоприятной окружающей среды». Это положение можно трактовать как требование проводить рекультивацию любой ценой, невзирая на соотношение затрат и приобретаемых выгод. Однако, в условиях рыночной экономики должен работать принцип, в соответствии с которым затраты на рекультивацию должны повышать ценность участка по сравнению с исходной ценой, ценность земли должна превосходить производственные затраты. Поэтому при разработке предложений по оцениванию состояния территории объектов МО РФ в Арктике с экологическим ущербом, накопленным в прошлом, следует ориентироваться на определение допустимой антропогенной нагрузки на экологическую систему региона. В качестве показателя антропогенной нагрузки рекомендуется использовать территориальные индексы $И_{б(т)}$ экологической безопасности и уровни предельно допустимой концентрации загрязняющих веществ $ПДК_в$. Вводятся три уровня опасности нарушения территории:

1 – удовлетворительный (ниже порога $П_1$),

2 – критический (между порогами $П_1$ и $П_2$),

3 – катастрофический (выше порога $П_2$), – в соответствии с которыми разрабатываются предложения по обращению с территориями с экологическим ущербом, накопленным в прошлом. Например, для малоопасных отходов $П_1$=10%, $П_2$=30%; для фитотоксичных отходов – $П_1$=0,5%. Если для участка с экологическим ущербом, накопленным в прошлом, индекс экологической безопасности $И_{б(т)}$ меньше порога $П_1$, экологическая обстановка может быть признана удовлетворительной и экономические соображения получают преимущество по сравнению с решением о полной ликвидации негативного воздействия на окружающую среду. Таким образом, результатом оценивания масштабов экологического ущерба территории (участкам) объектов МО РФ, нанесенного в прошлом, может быть принятие решения от полной ликвидации загрязнения до наблюдения за экологической обстановкой на объекте с постепенной ликвидацией опасных загрязнений естественным путем или путем очистки и рекультивации.

Для каждого конкретного объекта МО РФ с историческими загрязнениями способы решения проблемы ликвидации экологического ущерба, нанесенного в прошлом, с учетом объемов и характера финансирования определяются индивидуально на основе сформированных рекомендаций и предложений, используя предложенный перечень критериев. Предлагается принимать решение о реабилитации участков объекта МО РФ с экологическим ущербом, накопленным в прошлом, на средства государственного бюджета только в случаях угрозы здоровью населения и/или чрезвычайной ситуации. В остальных случаях с такой инициативой могут выступать региональные и муниципальные структуры, общественные организации и спонсоры. Данный подход может быть использован для объектов с историческим загрязнением в Арктике другой ведомственной подчиненности.

Мелентьев В.В., Черноок В.И., Ковалев Г.А., Мелентьев А.В., Смирнова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, АО «НИИ и ПКИ по развитиюи эксплуатации флота»
АО «Гипрорыбфлот»

ИСПОЛЬЗОВАНИЕ ГИС ДЛЯ ВСЕПОГОДНОЙ ДИСТАНЦИОННОЙ РСА ДИАГНОСТИКИ МОРСКИХ АКВАТОРИЙ КАК СРЕДЫ ОБИТАНИЯ ЛЕДОВЫХ ФОРМ МОРСКИХ МЛЕКОПИТАЮЩИХ (НА ПРИМЕРЕ ЛАПТЕВОМОРСКОГО МОРЖА)

Морж - один из крупнейших представителей морских млекопитающих, единственный современный вид семейства моржовых (Odobenidae), ареал которого имел когда-то циркумполярное распределение, занимая практически все прибрежье Российской Арктики. Однако вследствие сильнейшего антропогенного пресса и климатических изменений (сокращение площади льда) в последние десятилетия численность животных резко сократилась.

Выделяют три подвида моржа: тихоокеанский: (Odobenus rosmarus divergens Illiger, 1811) и атлантический (Odobenus rosmarus rosmarus Linnaeus, 1758), также лаптевоморский морж (Odobenus rosmarus laptevi Chapskii, 1940), занесенный в Красную Книгу России, комплексным аэрокосмическим исследованиям мест обитания которого и посвящена настоящая работа. Местом обитания последнего является район о. Котельный и так называемой Новосибирской стационарной полыньи, круглогодичное существование которой позволяет лаптевоморскому моржу не покидать район и в самые суровые зимы. К сожалению, в связи с труднодоступностью района и суровыми климатическими условиями наземные маммологические исследования здесь весьма затруднены и данные об экологии поведения этих животных весьма малочисленны.

Именно по этой причине инструментом для изучения состояния льда в районе Новосибирской полыньи нами были использованы радиолокационные снимки высокого разрешения со спутника Энвисат, для обработки которых использован пакет программ ГИС ArcGIS 10.1 Arc Map10., предназначенный для хранения данных, сбора информации в виде снимков, обработки данной информации, ее геопривязки и анализа в пространственно-координированных условиях о состоянии морской среды, а также информации, связанной с представлением в ГИС транспортных путей и объектов, позволяющий производить поиск, анализ и редактирование цифровых изображений, ввод в них дополнительной вспомогательной информации об исследуемых объектах и их состоянии. Используемые программы дают возможность управления базами данных, редактирования растровой и векторной графики, а также удобную способность анализировать изменчивость объекта во времени и под влиянием природных факторов и техногенных прессов.

К сожалению имеющиеся РСА сенсоры не позволяют обнаружить присутствие на льду даже таких крупных животных как морж, поэтому нами осуществляется косвенная оценка типа морского льда, а по его РСА сигнатуре определяется возможность присутствия на нем льда скоплений моржей. В докладе приводятся карты распределения морского льда, полученные на основании анализа последовательной серии РСА снимков, выполнявшихся в период 18-19 октября 2010 г., при этом более интенсивные цвета раскраски снимка соответствует более высокой вероятности присутствия морских животных.

В докладе также приводится итоговая сводка характеристик Айонского Арктического Океанического Массива (ААОМ), полученная по данным РСА съемки за период с 16 по 30 сентября 2010 г., и сведения о площади отдельных видов льда (S) осредненной в (км2), и по времени (по неделям), которые позволяют сделать заключение об особенностей миграций лаптевоморского моржа в указанный период.

Анализ РСА информации позволил в частности также выявить движение ААОМ на ЮЗ, в сторону Новосибирских о-вов, что приводит к образованию большого количества начальных видов льда и заставляет рекомендовать судоводителям смешение маршрутов движения в пролив Дмитрия Лаптева, поскольку обычный ледокольный путь через пролив Санникова оказывается опасным для жизнедеятельности моржей и других зимующих здесь ледовых форм млекопитающих. В тоже время смещение к северу от о-вов Анжу вызывает ряд экономических проблем, и прежде всего увеличение затрат на топливо.

Как показывает РСА съемка, движение ледоколов в исследуемом районе вызывает образование большого количества полыньей, трещин и разводьев, а так же образуют целые поля наслоенного однолетнего льда, что заставляет моржа возвращаться на берег, где он более уязвим для хищника, а где условия питания хуже. К тому же эта ситуация значительно увеличивает путь моржа к открытой воде. Таким образом, предлагаемый метод РСА мониторинга, позволяет документально фиксировать нарушения правил судоходства в районах массового скопления морских животных, и накладывать за это соответствующие финансовые взыскания и штрафы, что в итоге открывает возможность контроля и управления сохранением биоразнообразия арктической природы, и тем самым отодвинуть сроки полного исчезновения и вымирания ластоногих.

Рузанкина Ю.С., Васильев О.С., Парфенов В.А.
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ТЕХНОЛОГИЯ ПОВЫШЕНИЯ КОРРОЗИОННОЙ СТОЙКОСТИ СТАЛИ МЕТОДАМИ ФОТОНИКИ

Коррозия приносит огромные убытки, ее разрушительное действие мы видим во всем, что нас окружает, из-за коррозии выходят из строя машины, механизмы, различное оборудование. Большое количество аварийных ситуаций свидетельствует о том, что требования существующих нормативных документов, а также методы испытаний стали, недостаточны для обеспечения требуемой коррозионной стойкости и эксплуатационной надежности. Предохранение от коррозии и ее предупреждение – довольно трудоемкие и затратные мероприятия. Поэтому в настоящее время актуальна разработка дополнительных требований к сталям и методам их испытаний для повышения коррозионной стойкости и ресурса эксплуатации. На сегодняшний момент для повышения коррозионной стойкости металлов активно применяются процессы лазерного окисления. В связи с

этим, актуальным является как способ лазерного окисления металлов, так и определение режимов их обработки в каждом конкретном случае. Несмотря на то, что ранее уже были выполнены отдельные исследования по данной тематике все еще остается ряд проблем, требующих решения. Таким образом, исследование физико-химических процессов и механических свойств, происходящих на поверхности металлов при лазерном воздействии для защиты металла от коррозии являются также актуальной научной и практически важной задачей.

Работа посвящена исследованию возможности повышения коррозионной стойкости металла за счет обработки поверхности стали непрерывным излучением волоконного лазера на длине волны λ=1064 нм. Авторами работы проведены тестовые испытания и определены параметры обработки, определяющие высокую антикоррозийную защиту поверхности облучаемого металла. Воздействие лазерного излучения на поверхность стали поспособствовало изменению химического состава. Было обнаружено появление таких химических веществ как Al, F, O. Присутствие F было изначально в исследуемой марки стали, но воздействие лазерного излучения значительно увеличило его концентрацию в металле от 0.01 атом. % до 5,24 атом. %. В процессе исследования было зафиксировано изменение шероховатости поверхности стали со значения 3.66 до 2.66. Оптимальные режимы обработки поверхности стали были получены при плотностях мощности q0=93,5÷95,3 Вт/см2. Полученные результаты найдут широкое применение в промышленности, стоит отметить, что исследования находятся на начальном этапе и будут продолжены для более детального анализа.

Смирнов Л.В., Гришканич А.С., Елизаров В.В., Кащеев С.В.
Россия, Санкт-Петербург, Университет ИТМО

ОСНОВНЫЕ ПОДХОДЫ К РАЗРАБОТКЕ ЛИДАРА ДЛЯ МОНИТОРИНГА ПОВЕРХНОСТИ МАРСА

Как известно, человечество издавна интересуется красной планетой. С течением времени и развитием техники и технологий исследование Марса стало более детальным. Детальный анализ позволяет с высокой точностью определить пригодность этой планета, для потенциального ее терраформирования. Одним из решающих факторов является присутствие воды на красной планете. В недавнем прошлом на поверхности Марса была обнаружена водянистая суспензия, благодаря спектральному анализу были получены ее основные компоненты. С помощью передовых технологий в лидаростроении становится возможным исследование поверхности Марса на значительном расстоянии. Используя передовую технологию, значительно сокращается время затраченное на поиск воды и увеличивается точность проводимых исследований.

Хафизов Н. Ф., Гришканич А.С., Рузанкина Ю.С.
Россия, Санкт-Петербург, Университет ИТМО

ЛАЗЕРНОЕ ОБЕЗЗАРАЖИВАНИЕ ВОДЫ

Лазерное обеззараживание воды – современный развивающийся способ, решающий проблему уничтожения бактерий и вирусов в воде. Данный метод очень похож по реализации с ультрафиолетовым обеззараживанием при помощи ртутных ламп. Они оба используют ультрафиолетового излучения. А преимущество – возможность обеспечения плотности мощности, достаточной для уничтожения любых спорообразующих вирусов. Суть метода заключается в использовании полупроводниковых лазерных диодных сборок, либо твердотельного лазера на определённом участке водопровода. КПД лазерных установок превосходит КПД ртутных ламп. Малые вес и габариты позволяют масштабировать использование установок, начиная от бытовых нужд, заканчивая скотоводческими фермами.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

ПРИНЦИП 80/20 И ЕГО РАЗВИТИЕ ДЛЯ СМЕЩЕННЫХ ОДНОРОДНЫХ ПРОЦЕССОВ

Известный принцип «80/20» своим чуть менее 120-летним существованием не только подтверждает свою общность, повторяемость и практическую значимость, но и, по-прежнему, в определенном смысле этого слова остается неисчерпаемым. Как минимум, позволяет к нему все чаще обращаться в поисках срытых ресурсов развития в различных предметных областях.

Эмпирическое правило, названное в честь итальянского экономиста и социолога Вильфредо Парето (1848-1923), выявившего в 1897 г. частную экономико-социальную закономерность, в наиболее общем и популярном виде сегодня формулируется как «20 % усилий/временных затрат дают 80 % результата, а остальные 80 % усилий/времени — лишь 20 % результата».

Данный принцип В. Парето сегодня используется как базовая установка (замысел, концепция) в анализе факторов эффективности какой-либо деятельности и оптимизации её результатов: правильно выбрав минимум самых важных действий, можно, как известно, быстро получить значительную часть от планируемого полного результата. При этом считается, что дальнейшие улучшения неэффективны и являются избыточными, а, значит, по использованию ресурсов необоснованными.

Сегодня к 120-летию существования принципа Парето назрела необходимость поиска принципа связи результатов и усилий не для одного процесса, а одновременно для нескольких анализируемых (измеряемых, контролируемых) процессов, в том числе однородных (с подобными статистическими характеристиками) и неоднородных. А также процессов, начинающихся одновременно (синхронных по признаку несмещенности их начала) и со смещением по времени начала (асинхронных). Причем, критерием, по-прежнему, будем считать возможность (вероятность) получения результата в зависимости от приложенных усилий/временных затрат.

С этой целью проанализирован типовой вариант графической интерпретации и границы применимости принципа Парето для одного процесса с распределением случайной величины приведенного вида, а также приведены результаты вариантных расчетов параметров распределения «Результат (усилия)» для двух и трех однородных смещенных (асинхронных) процессов.

Это позволило сформулировать соответственно принципы «5/94/35» и «5/98/25». Их существо сводится к следующему: при двух однородных процессах, смещенных во времени (по усилиям) на 5 %, с 1 %-погрешностью 94 %-результат достигается в первые 20 % времени (усилий), а практически полный (с погрешностью 1%) 100 %-результат – в первые 35 % времени (усилий).

Для трех однородных процессов соответственно 5 %-смещение процессов в первые 20 % времени (усилий) достигается 98 %-результат, а в первые 25 % времени (усилий) – практически 100 %-результат.

Приведены многочисленные характерные варианты интерпретации принципа Парето «80/20» в самых различных предметных областях, а также в его развитие принципов «5/94/35» и «5/98/25».

Показано, что эффективным алгоритмом планирования процессов управления следует считать включение в план кроме конечных 100 %-результатов в заданные сроки также поэтапных контролируемых показателей в соответствии с принципом Парето типа «80 %-результатов в 20 %-срок». А также - считать целесообразными критериями конкурсного (тендерного) сравнения конкурентные показатели типа «Минимальный срок достижения 80 %-результата».

В отличие от традиционного критерия конкурсного сравнения «Минимум ресурсных затрат при заданном качестве» данный критерий предусматривает обязательный количественно измеряемый (квалиметрический) контроль качества результата, что на практике часто упрощается и опускается.

Сегодня, при определенном дефиците конструктивных путей решения национальной проблемы повышения технологического уровня создаваемых технических комплексов и систем, обеспечения их конкурентоспособности, в качестве одного из перспективных путей рекомендуется использовать рассмотренные варианты обобщения принципа Парето «20/80» для смещенных (однородных и неоднородных) процессов в вариантах «5/94/35», «5/98/25» и аналогичных.

Это позволит существенно повысить в дополнение к рассмотренным разнородным вариантам качество и результативность организационно-технических алгоритмов управления современными сложными эргатическими системами.

Отмечено, что принцип Парето «80/20» и варианты его развития «5/94/35», «5/98/25» лишь обосновывают необходимость концентрации всегда ограниченных ресурсов системы на ограниченном участке действий вместо их привычного распыления по множеству направлений. Это помогает определить именно тот участок, где можно рассчитывать на максимальный результат от своих усилий.

Выполненный анализ известного принципа В. Парето «20/80» для нескольких однородных процессов позволил выявить новую возможность повышения качества управления сложными эргатическими системами за счет их взаимного смещения в пространстве усилий или времени.

Приведены результаты количественной оценки и обобщения выявленных принципов для широкого круга приложений с принципиальной возможностью повышения результативности групповых процессов.

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

МОДЕЛЬ ОЦЕНКИ КАЧЕСТВА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Анализ и синтез систем обеспечения информационной безопасности (ИБ) объектов информатизации в свете комплекса требований государственных, ведомственных и корпоративных регламентов по широкому спектру специализаций предусматривает объективную качественную и количественную оценку уровня обеспечения защищенности информационных ресурсов (ИР).

Сегодня, в условиях решения национальной задачи обеспечения конкурентной способности и импортозамещаемости разрабатываемых технологий и комплексных систем защиты информации (КСЗИ), это требование становится особенно актуальным и востребованным. Прежде всего, в интересах концентрации национальных средств и компетенций специалистов при решении методологически и технологически сложных задач обеспечения качества современных автоматизированных систем в защищенном исполнении (АСЗИ), средств информационного противодействия (средств ИПД) и информационного противоборства (ИП) в целом.

На пути решения этой проблемы к числу традиционно неоднозначных по эффективности задач относятся вопросы создания методики комплексной оценки и ранжирования уровня качества (квалиметрической оценки) обеспечения защищенности ИР и ИБ в целом сложных эрготехнических и эргатических систем, а также обеспечения объективности оценивания АСЗИ с использованием подобных методик. Так, даже по традиционным критериям оценивания конфиденциальности, доступности и целостности ИР АСЗИ сегодня единых (с учетом инвариантности к специфике решаемых задач) методик по существу нет. Следовательно, нет условий для обеспечения ранжирования и оценки конкурентной способности технологических решений (ТР) при одновременном наличие широкого спектра требований стандартов, руководящих документов и регламентов ФСТЭК. Более того, имеются утверждения, что прямой перенос понятий ИБ в виде конфиденциальности, доступности и целостности в киберфизические системы (сочетающие вычислительные и исполнительные компоненты) невозможен.

С другой стороны, «непреодолимым» остается при проведении сертификационных и других видов испытаний «защищенность от негативного влияния субъективных (человеческих) факторов». Уже эти два обстоятельства существенно сдерживают, а в целом ряде случаев и не позволяют производить объективную сравнительную квалиметрическую оценку существующих, разрабатываемых и перспективных ТР, АСЗИ и систем обеспечения ИБ, ИПД и ИП в целом. Это, естественно, с одной стороны, снижает мотивацию специалистов, а, с другой стороны, снижает в целом качество создаваемых АСЗИ и приводит к неэффективному использованию национальных ресурсов (финансовых, трудовых, технических, материальных и др.). Но, самое главное, не позволяет обеспечить надежное и устойчивое противостояние (ИБ и ИПД) и противоборство в информационной сфере (ИП) в целом.

В докладе представлены две технологии и два программных комплекса, позволяющие в определенной мере продвинуться на пути названных проблем, включая:

1. Программный комплекс многокритериального квалиметрического оценивания сложных АСЗИ, инвариантный к специфике решаемых задач (ПК «МКО-И»). Он обеспечивает: оценку агрегированного (сводного) показателя качества (АПК) с соответствующими оценками свойств и групповых показателей качества (ГПК) АСЗИ в составе АСЗИ; объективность производимых оценок частных показателей качества (ЧПК) АСЗИ экспертами за счет создания условий их взаимной независимости; конфиденциальность представляемых оценок и их взаимную обработку; учет уровня

компетентности экспертов и значимость соответствующих критериев; полную защищенность получаемых данных от администраторов АСЗИ и других участников оценивания.

2. Программный комплекс оценивания конфиденциальности, доступности, целостности ИР АСЗИ с комплексной оценкой уровня ИБ по критерию АПК ИБ (ПК «АПК АСЗИ»). Он обеспечивает: многокритериальную оценку ЧПК и ГПК АСЗИ отдельно для аппаратно-программных (АПС) и программных средств (ПС) в соответствии с действующими регламентами, включая ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»; возможность учета специфики АПС, ПС, структуры АСЗИ и распределения ИР по её элементам при методической инвариантности к специфике элементов АСЗИ; графическую визуализацию влияния свойств и параметров элементов АСЗИ на их ГПК и АПК; информационно-справочную поддержку экспертов в части используемых терминов и их системной взаимосвязи.

Предложенный подход и методика оценки качества АСЗИ в составе ОМТИ, ПК «МКО-И» и «АПК АСЗИ» существенно снижают негативное влияние субъективного (человеческого) фактора при анализе параметров и требований к АСЗИ. Кроме того, позволяют ранжировать АСЗИ по интегрированному значению уровня качества, адекватнее оценить их роль и место, а также квалиметрически обоснованно решать задачи системного анализа, синтеза и оптимизации как средств, так и АСЗИ в целом, включая использование в рамках так называемой системы ранговой партнерской сертификации (СПРС). В том числе, как показано в докладе, для класса корабельных центральных координирующих систем управления в защищенном исполнении, систем автоматизированной информационно-аналитической и интеллектуальной поддержки решений судоводителей, автоматических систем поддержки (оптимизации) решений и управления (АСПРУ) техногенных морских объектов повышенного риска.

Алексеев А.В., Воробьев В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, Санкт-Петербургский институт автоматизации и информатизации РАН

20 ЛЕТ КОНЦЕПТУАЛЬНОГО И ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ ПРОБЛЕМ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Понятия «информационное противоборство» (ИП), «информационная война», «ведение боевых действий в едином информационно-коммуникационном пространстве» или в современном варианте «сетецентрическая война» рассматриваются сегодня, как система боевых противоборств с применением воинских формирований, как модель применения своеобразных устройств, подключенных к единой сети.

В этом, собственно, и проявляется эффект синергизма ИП, когда целое представляет нечто большее, чем сумма его частей. Этот системный (синэргетический, эмерджентный) эффект от совместного действия объединенных в сеть средств вооруженной борьбы по совокупному результату превышает сумму эффектов от применения тех же средств ведения вооруженной борьбы по отдельности.

Для достижения эффекта синергизма ИП необходима, прежде всего, совершенная «цифровизация» самой системы управления. Но это только начало пути, так как неотъемлемым условием реализации новой концепции становится развертывание компьютерных сетей и обеспечивающих информационных технологий, то есть современных аппаратных и программных средств, средств обеспечения автоматизации процессов подготовки и принятия тактических, оперативно-тактических, оперативных и оперативно-стратегических решений, хранения, обработки и доведения информации и многого другого.

Причиной постановки данной темы анализа послужил 20-летний период, прошедший с первой постановки авторами проблемы анализа возможностей, развития технологий и концепций ведения информационных войн в 1995 г. в процессе подготовки к V Санкт-Петербургской международной конференции "Региональная информатика-96 ".

Выполнен анализ 20-летнего периода концептуального и технологического развития сил и средств ведения информационного противоборства от концепций информационных войн до современного их варианта в форме сетецентрических войн. Показано, что только на основе широкомасштабных, хорошо скоординированных процессов информационного противоборства с использованием возможностей современных информационных технологий можно фактически парализовать систему управления силами и оружием противника без нанесения ему невосполнимых ресурсных потерь. Сформулированы проблемы и реальные пути преодоления отставания в области информационного противоборства.

В виду особенностей ИП (современной его концепции в форме сетецентрического (СЦП) противоборства), а, именно, создания удаленного управления от места события необходима, прежде всего, подробная и адекватная картина представления информации, учитывающая особенности восприятия информации операторами и лицами, принимающими решения (ЛПР), а также для

возможности принятия ЛПР своевременного решения. Поэтому специфическими для задач ИП требованиями к силам и средствам его обеспечения могут быть названы, прежде всего:

– превосходство в концепциях и способах ведения информационных операций и информационно-боевых действиях, как отмечалось еще 20 лет назад, на основе, прежде всего, обеспечения превосходства в оперативно-тактико-технических свойствах (ОТТС) и характеристиках используемых сил и средств ведения ИП, а также превосходства в целом используемых информационных технологий (ИТ). Решение этой системной задачи предусматривает разработку и приоритетную реализацию соответствующей национальной программы;

– превосходство в целях и средствах ИП на основе соответствующих сетевых сил и средств управления и связи, разведки, средств поражения, личного состава и обеспечения. Причем, приоритетным и первостепенным направлением, как показывает опыт, следует считать совершенствование форм и методов организационного управления с максимальным обеспечением прозрачности информационного поля управления на основе современных технологий открытой (прозрачной) оптимизации проектных и управленческих (для ЛПР) решений (ПУР). При этом, достигаемыми целями ИП должны быть:

– ликвидация оперативности использования информации потенциальным противником (ПП) на основе концепций массирования информационных потоков, информационного удушья, стимулирования отказа от управления, информационного психоза, информационного террора и диверсий, рефлексивного управления и др.;

– ликвидация достоверности получаемой ПП информации на основе концепций обмана ПП, перераспределения информации, создания многовариантной виртуальной обстановки, электромагнитного, биологического разрушения носителей и др.;

– ликвидация устойчивости добывания ПП информации на основе концепций информационного инфицирования, информационных взрывов, компьютерных диверсий, информационно-психологического обеспечения различных видов ИП и др.;

– ликвидация скрытности добывания и использования информации ПП на основе концепций информационной подсветки, демаскирования, деструктивных действий и др.;

– ликвидация непрерывности получения информации ПП на основе концепций информационного блокирования, активации информационных закладок, информационного разрушения систем адаптации, управления темпом информационного обмена и др.;

– ликвидации информационного структурирования систем ПП на основе концепций информационного вскрытия (подсказки) уязвимых элементов, управления информационной прозрачностью общества и сред взаимодействия и др.;

– превосходство в средствах автоматизированной (преимущественно - автоматической) многомерной комплексной визуализации и обработки информации. Именно многомерность представления информации ЛПР позволяет, с одной стороны, отображать весь «огромный» массив данных, поступающий на автоматизированное рабочее место ЛПР, а, с другой стороны, максимально полно учитывать современные технологические возможности, аспекты и особенности средств в «комфортном» сопряжении с психофизиологическими возможностями ЛПР;

– превосходство в силах и средствах защиты информационных ресурсов ведения ИП и, в первую очередь, верхних степеней защищенности информации (критической информации). Как по традиционным критериям конфиденциальности, доступности, целостности, так и по основным критериям управления силами и средствами, свойствам используемой информации – её оперативности (своевременности), достоверности, устойчивости, скрытности, непрерывности, а также интегральных её критериев - ценности информации и безизбыточности. В этой связи особое значение приобретают средства и технологии обеспечения информационной маскировки и дезинформации противника, как специфических форм оперативного (тактического, оперативно-тактического, оперативно-стратегического, стратегического) искусства ведения ИП (СЦП);

– превосходство в силах и средствах информационных вторжений с совершенным организационно-техническим арсеналом ведения повседневных информационно-боевых действий, информационных атак, информационных операций, информационных сражений и других форм. При этом весьма значимым следует считать непрерывное накопление опыта ИП, его актуализации, в том числе в процессе специальной подготовки, учебно-тренировочной работы и проведения комплексных учений по ИП;

– превосходство в теоретическом и научно-методическом обеспечении ведения ИП, подготовки и переподготовки специальных кадров, как принято сегодня их называть – кибервоинов. Особое значение в этом контексте должно принадлежать проведению специализированных научно-исследовательских и опытно-конструкторских работ, обеспечивающих соответствующие приоритеты развития. В том числе на базе системно-аналитических обобщений опыта проведения различных видов и форм ИП в ходе международных конфликтов и войн последнего периода – Египет, Фолкленды, Югославия, Украина, Ирак, Афганистан, Ливия, Сирия и других.

Выполнен ретроспективный анализ 20-летнего периода развития концепций и технологий ИП от концепций информационных войн (в том числе объявленной в известной сегодня Директиве объединенного командования начальников штабов НАТО № 30, 1993 г.) до концепций сетецентрических войн. Анализ показывает все возрастающее значение обеспечения информационной безопасности (ИБ) объектов информатизации, активного информационного противодействия (ИПД) и ИП в целом, но, кроме того, и определенные признаки продолжающего отставания в этой области.

Особое внимание в этих условиях сегодня, по нашему мнению, следует уделять, прежде всего, развитию теории и практики ведения ИБ, ИПД и ИП в целом, вариантному концептуальному и исследовательскому проектированию АСЗИ с широким применением средств имитационного и игрового моделирования. Это требует неотложного решения комплекса методических вопросов количественной оценки конкурентной способности и импортозамещения средств ИП с переходом к технологиям сертификации соответствия качества, создания сетевых полигонов моделирования процессов ИП, СЦП, создания центров освоения технологий ИП и ряда других неотложных задач.

Алексеев А.В., Левадный И.В., Мусатенко Р.И., Смольников А.В., Сус Г.Н., Ушакова Н.П.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, АО «Концерн «НПО «Аврора»

ТЕХНОЛОГИЯ И ПРОГРАММНЫЙ КОМПЛЕКС СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ СУДОВОДИТЕЛЯ В СЕТЕВОМ ИСПОЛНЕНИИ (ТиПК «СПРУ-С»)

Презентуется «Технология и программный комплекс Системы поддержки принятия решений и управления судоводителя в сетевом исполнении (ТиПК «СПРУ-С»)», заявленные 28.09.2016 группой авторов в Открытом конкурсе «Конкурентно способное технологическое решение в классе систем информационной поддержки решений по управлению сложными эргатическими системами повышенного риска (КСТР-2016)».

Заявленные ТиПК «СПРУ-С» базируются на ранее разработанной в 2012 - 2014 г.г. технологии СПРУ, созданной в ходе выполнения ряда НИР и ОКР по Федеральной целевой программе «Развитие гражданской морской техники» на 2009-2016 годы» (утверждена постановлением Правительства РФ от 21 февраля 2008 г. № 103) и зарегистрированного ПК в ФСИС за № 2014614620, 29.04.2015.

В отличие от базового варианта реализации данной информационной технологии и ПК (впервые были представлены в «КСТР-2014» в варианте ТПК «ИСППР») в заявленном варианте решена задача сетевого информационно-коммуникационного обеспечения автоматизированных рабочих мест (АРМ) операторов СПРУ (командира корабля, капитана судна, вахтенного офицера, вахтенного помощника капитана, командира БЧ-5, старшего электромеханика и т.д.).

Проведенные комплексные испытания ПК «СПРУ-С» в сочетании с результатами ТПК «ИСППР» показали следующие преимущественные особенности и основные системно-технические характеристики заявляемого технологического решения и ПК:

1. Максимальный (>90%) охват процессов обеспечения безопасности эксплуатации (ОБЭ), локализации аварийных ситуаций и аварий (ЛА), а также борьбы за живучесть (БЖ) корабля, судна контуром автоматического сетевого управления.
2. 100%-ное комплексное (агрегированное) использование объективных источников данных о техническом состоянии корабля, судна (более 2 тыс. датчиков).
3. Малоизбыточная (<10%) динамическая ретроспективная визуализация данных с автоматической локализацией и видеомониторингом аварийных зон.
4. Адаптивное прогнозирование развития АС по времени (до 30 минут) и по динамике уровней (10-15%), позволяющие качественнее готовить, обосновать и принимать управленческие решения.
5. Минимизация числа циклов принятия решений более, чем в 3 раза.
6. Текстовая логически сжатая форма представления проектов управленческих решений по ОБЭ, ЛА и БЖ с их автоматическим доведением после принятия решения до АРМ операторов с автоматической аудио- , фото- и видео-поддержкой.
7. Количественное обоснование управленческих решений с ранжированным представлением возможных альтернативных вариантов.
8. Регистрация, контроль и сетевой мониторинг эффективности реализации принятых решений с возможностью их своевременной корректировки.
9. Непрерывный (с циклом от 2 минут) контроль, мониторинг и регистрация процесса принятия решений, минимизация возможности «пассивного» и ошибочного управления ОБЭ, ЛА и БЖ вплоть до «отказа (потери) от управления».
10. Оценка, прогнозирование и мониторинг критичности развития аварийных ситуаций.
11. Пространственная автоматическая локализация факторов возникновения АС.
12. Сетевое информационно-коммуникационное обеспечение СПРУ-С.
13. Конкурентная способность в сравнении с базовым вариантов не менее 54% (материалы конференции «МОРИНТЕХ-ПРАКТИК. Информационные технологии в судостроении – 2016», с. 75).

14.Перспективность развития в сравнении с базовым вариантом более 44% (там же).

15.Оценка объема затрат по реализации ТиПК «СПРУ-С» - порядка 2,8 млн. руб.

Обсуждаются наиболее значимые и проблемные вопросы архитектуры ПК «СПРУ-С», его программно-алгоритмического обеспечения, опыт реализации комплекса типовых сценариев ОБЭ, ЛА и БЖ, результаты имитационного и численного моделирования, а также наиболее важные методологические вопросы и результаты с целью дальнейшего развития технологии и ПК «СПРУ-С» в различных задачах и условиях. Приведены результаты обобщения опыта и коллективного осмысления полученных теоретических и практических знаний по данной большой и сложной проблеме.

Алексеев А.В., Карпов А.Е., Мусатенко Р.И., Потехин В.С., Худобородов Е.Ф.
Россия, Санкт-Петербург, Военный учебно-научный центр ВМФ «Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова»

ОТ МОНИТОРИНГА ДАННЫХ К МОНИТОРИНГУ ПРОЦЕССОВ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Для оценки технического состояния объектов морской техники (ОМТ) традиционно используется целый комплекс каналов контроля, обработка данных которых позволяет сделать заключение о соответствии условий и режима эксплуатации ОМТ заданным требованиям. При этом, как правило, на монитор операторов выводятся текущие состояния ОМТ по каждому из каналов контроля, либо агрегированной группы каналов, отражающих соответствующее свойство ОМТ.

При таком подходе имеет место определенная избыточность системы мониторинга обстановки, обусловленная, как правило, значительным объемом информации в каждом из каналов контроля, так как традиционно к этим каналам предъявляются достаточно высокие метрологические требования.

В условиях современной тенденции резкого роста структурной и функциональной сложности ОМТ и соответствующих каналов контроля объем данных о состоянии ОМТ существенно возрастает. При этом объем данных, предъявляемых операторам для принятия управленческих решений, в целом ряде случае либо находится на грани психофизиологических границ по возможностям её приема, обработки и анализа, либо вообще эти границы превышает. Аналогичная ситуация имеет место и для агрегированных каналов, а эргономические требования к ОМТ все чаще становятся критичными при проектировании. Естественно, критичность этой ситуации для условий экстремальных, аварийных ситуаций и аварий, а, тем более, для условий борьбы за живучесть корабля, судна резко обостряется.

Одним из путей решения этой актуальной проблемы, по нашему мнению, следует считать переход от «измерительной парадигмы» построения систем контроля технического состояния ОМТ к «процессной парадигме». Её существо сводится к измерению, обработке и контролю состояния ОМТ не по отдельным и агрегированным каналам контроля, а к измерению, обработке и контролю процесса в целом с автоматическим анализом и контролем динамики процессов.

Для реализации этого подхода представляется целесообразным ввести новые параметры оценки и контроля процессов типа:

- соответствие протекающего и контролируемого процесса заданным границам варьирования качества, например, с типовыми уровнями «Соответствует требованиям», «Угроза невыполнения требований», «Невыполнение требований», «Угроза потери качества и контроля». При этом оценку уровня качества функционирования ОМТ, как показано в ряде исследований, целесообразно выполнять по гармоническому алгоритму агрегирования частных показателей качества;
- соответствие протекающего и контролируемого процесса заданным границам динамического варьирования, например, с типовыми уровнями «Устойчивое функционирование», «Угроза потери устойчивости», «Потеря устойчивости», «Угроза неуправляемости». При этом, оценку уровня устойчивости качества функционирования ОМТ можно выполнять, например, по критерию длительности отказа (восстановления) критических элементов ОМТ;

В ходе реализации данной «процессной парадигмы» представляется целесообразным вместо вывода на экран оператора данных о состоянии ОМТ и их изменении представлять данные о процессе функционирования ОМТ в целом в координатах «Качество-Устойчивость». При этом, число возможных значений составит 4*4=24, т.е. для передачи этих данных потребуется всего лишь канал в 4 бит.

Наряду с существенным сокращением объема информации при переходе от мониторинга данных к мониторингу процессов ОМТ имеет место также, в определенном смысле, повышение комфортности и информационной прозрачности для операторов при анализе ими отображаемой в этом формате информации о состоянии ОМТ и принятии ими управленческих решений. Кроме того, при прогнозировании развития обстановки, например, на основе аппарата регрессионного анализа.

Причем, практически полная автоматизация процессов диагностирования состояния ОМТ фактически исключает возможность отказа от принятия решения оператором, так как, например, предельное состояние «Угроза потери качества и контроля» при «Угрозе неуправляемости» является настолько критическим, что отказ от принятия решения оператором равнозначен «саботажу системы

управления». С учетом регистрации состава каждого цикла управления эта ситуация равнозначна такому варианту решения системы управления, как «отказ оператора от принятия решения».

Показано, что обязательным элементом подобных автоматизированных систем управления при реализации данной парадигмы следует считать систему поддержки и принятия решений, на которую возлагается практически вся ответственность за решение информационно-аналитической задачи. И это не может вызывать сомнений, так как тенденция роста сложности современных управляемых систем фактически приводит к ситуации в этих условиях практической невозможности своевременного (оперативного) и малоошибочного анализа и принятия управленческих решений только оператором.

Перенос же «центра ответственности» на «автоматический сегмент» управления ОМТ и тренд к роботизации ОМТ, можно полагать, неизбежным при поиске направлений и реализации требований по обеспечению безопасности мореплавания и обеспечивающих её объектов морской техники.

Поляничко В.В., Алексеев А.В.
Россия, Санкт-Петербург, ООО «ЦНИиР «Кристалл», НП «ИАП БЖКС»

КОНЦЕПЦИЯ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО МОНИТОРИНГА И ПРОЦЕССНОГО УПРАВЛЕНИЯ СТРУКТУРОЙ И КАЧЕСТВОМ ЖИЗНЕННОГО ЦИКЛА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Существующая потребность в контроле соответствия заданным требованиям показателей качества, эффективности функционирования (ЭФ), перспективности развития (ПР) и конкурентной способности (КС) объектов морской техники (ОМТ) и управлении ими на протяжении всего жизненного цикла обусловлена так же постоянно растущими затратами на проектирование, строительство, эксплуатацию кораблей и судов, как следствие, стремлением эти затраты снизить. Это привело к бурному росту и развитию в последнее время различных систем информационной поддержки управленческих решений (СИП), включая СИП технического обслуживания и ремонта современных ОМТ, а также управления их жизненным циклом в целом (СИП ЖЦ ОМТ).

Разработка и освоение подобных средств, в том числе в классе PLM-технологий и систем автоматизации управления этапами ЖЦ ОМТ, в современных условиях является важным направлением развития корабельного и судового состава флотов, обеспечения их сбалансированного и перспективного развития, конкурентной способности на ведомственном, национальном и мировом рынках.

В дополнение к известным сегодня PLM-технологиям и PLM-системам (включающих САПР (в составе CAE, CAD, CAM), PDM, SCM, CPC, АСУП (в составе ERP, MRP, MRP II, SCM), MES, АСУТП (в составе SCADA, CNC), CRM, IETM, ITIL), представляющим собой, как правило, системы управления базами данных, нами предлагаются к рассмотрению СИП ЖЦ, которые решают в качестве основных задачи информационно-аналитической и интеллектуальной поддержки принятия решений при управлении качеством, ЭФ, ПР и КС ОМТ и его ЖЦ, далее - СПРУ ЖЦ ОМТ.

При этом ключевыми в составе таких СПРУ-ЖЦ ОМТ являются когнитивные модели формирования проектов управленческих решений на базе агрегирования частных, групповых и модельных показателей качества многочисленных функциональных элементов ОМТ. Именно поэтому применительно к ЖЦ ОМТ в целом введение этих функций в составе СПРУ-ЖЦ ОМТ позволит перейти на качественно новый уровень количественного измерения (квалиметрической оценки) и непрерывного наблюдения (мониторинга) на протяжение всего ЖЦ ОМТ ключевых системных показателей качества не только технической компоненты ОМТ с использованием всего массива данных PLM-систем, но и самой трудно реализуемой компоненты автоматизации - организационно-технического управления с показателями системного анализа и синтеза эффективных (конкурентно способных) и оптимальных (лучших из возможных альтернативных) вариантов управленческих решений по обеспечению ЖЦ ОМТ.

Концептуальными принципами построения и использования подобной СПРУ организационно-технического мониторинга и процессного управления структурой и качеством ЖЦ ОМТ, по нашему мнению, должны быть: принцип квалиметрической, полимодельной, многокритериальной и безизбыточной (четырех-уровневой по отношению к заданным требованиям) оценки качества ОМТ, а также оценки качества выполнения проектных (плановых) мероприятий; принцип непрерывного наблюдения (мониторинга) состояния ОМТ, каждого из элементов ЖЦ ОМТ и их прогнозирования на всем интервале ЖЦ с дополнительной оценкой уровней качества, ЭФ, ПР и КС развития ОМТ в целом и контролем допустимости отклонения от проектных значений; принцип квалиметрического анализа, синтеза и оптимизации проектов управленческих решений с их представлением лицу, принимающему решение (ЛПР), в системно-завершенном (целостном) и максимально удобном (комфортном) виде для ЛПР; принцип мониторинга и контроля качества решений ЛПР всех уровней с дополнительной оценкой их своевременности, качества, ЭФ (реализации), ПР (результативности, валидности) и КС (выигрышности).

Это обеспечивается широкой и глубоко-интегрированной по горизонтали и вертикали базой исходных данных, формированием и представлением ЛПР в непрерывном (мониторинговом) режиме вариантов и результатов его управленческой деятельности в сравнении с заданными (проектными) требованиями. Кроме того, представлением ЛПР прогноза изменения качества ОМТ с максимально-возможным упреждением (практически и впервые на всем интервале ЖЦ) при условии принятия рекомендуемых управленческих решений.

При этом рекомендуемое (оптимальное в каждом цикле управления) решение автоматически определяется по соответствующему алгоритму на основе принятых требований с учетом ситуационных данных, прогноза их организационно-технического развития, включая обеспечение требований безопасности эксплуатации, результативной локализации аварийных ситуаций, а также борьбы за живучесть ОМТ.

Реализация предложенной концепции предусматривает мониторинг, прежде всего, системных показателей качества ОМТ, его ЭФ, КС и ПР, определяемых через измеряемые частные (нижний, первичный уровень), групповые, модельные и агрегированный (верхний уровень) показатели качества. Тем самым достигается комплексный контроль качества ОМТ и его ЖЦ по всей совокупности исходных данных процессного управления в зависимости от принятой, реализуемой и корректируемой при необходимости модели структурного и процессного представления ОМТ и его ЖЦ с соответствующими количественными характеристиками.

При этом, ожидаемым эффектом реализации предлагаемой концепции СПРУ-ЖЦ следует считать: практическую реализацию требований по обеспечению системной прозрачности управления ЖЦ ОМТ с соответствующей минимизацией влияния в контуре управления негативных свойств ЛПР (пресловутого «человеческого фактора»); масштабируемость СПРУ-ЖЦ (возможность структурно-функционального наращивания и адаптации в зависимости от масштаба задач управления и их изменения); интегрируемость (возможность информационно-технического и аппаратно-программного сопряжения) с существующими системами автоматизированного управления, включая системы класса PLM; сокращение времени на принятие решения ЛПР (повышение оперативности управления); преимущественное принятие наилучших из возможных (оптимальных) решений и практическое исключение возможности принятия ошибочных решений (повышение качества управления); повышение цикличности управления (возможность увеличения числа циклов принятия оптимальных решений в заданное время); повышение комфортности и производительности управленческого труда ЛПР, в том числе по критериям качества, ЭФ, ПР; снижение затрат на создание и эксплуатацию ОМТ и, как следствие, стоимости их ЖЦ; повышение уровня качества, КС и ПР ОМТ на всех стадиях жизненного цикла.

Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, АО «Концерн «НПО «Аврора»

РАЗВИТИЕ МЕТОДОЛОГИИ ОМКАР И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ РАЗВИТИЕМ КРИТИЧЕСКИХ МОРСКИХ ОБЪЕКТОВ

Численное моделирование, анализ факторов и тенденций развития, научно-методическое обоснование практических рекомендаций по оптимизации проектных и управленческих решений в обеспечение перспективного развития критических морских объектов в настоящее время становится все более востребованным. Обусловлено это наряду с потребностями повышения достоверности прогнозирования конкурентной способности концернов и предприятий на рынке продуктов и услуг также потребностью повышения достоверности обоснования перспективности развития, прежде всего, критических морских объектов (КМО).

Более того, сегодня практически созданы условия для перехода к апостериорному анализу качества принятых ранее решений, трендов развития конкурентов и участников рынка в целом и, даже, мониторинга развития рынка. Особое значение сегодня совершенствование методик и технологий подобного анализа имеет для отраслевых национальных и международных (мировых) рынков.

В развитие известных методов системного факторного SWOT-анализа и его модификаций в вариантах STEEP, PETS, PETSE, STEEPV, STEPLE-методов в последние годы активное развитие получили так называемый обобщенный метод квалиметрического анализа факторов развития (ОМКАР), а также технология информационно-аналитической и интеллектуальной поддержки управления развитием КМО и, в целом, объектов морской техники и морской инфраструктуры (ОМТИ).

Ключевыми преимуществами ОМКАР и реализующей его технологии является переход от анализа данных к анализу процессов с оценкой, анализом и контролем трендов состояния ОМТИ, что особенно важно для КМО в связи с спецификой масштабов и значений возможных рисков.

Как показывают полученные результаты численного моделирования с использованием ОМКАР применительно к реальным условиям и количественным оценкам развития одного из лидирующих в

стране акционерных обществ в области автоматизации КМО, подобный анализ позволяет успешно вскрывать и прогнозировать макропроцессы развития. Более того, синтезировать на их основе решения долгосрочного развития с учётом широкого спектра специфических особенностей внутренних и внешних факторов, характерных сегодня для отрасли морского приборостроения страны в целом,.

В дальнейшее развитие ОМКАР и его технологии реализации предложены, обоснованы и на основе анализа результатов численного моделирования обсуждаются:

- предложения по систематизации и типизации систем критериев и матриц критериальных предпочтений для соответствующих кластеров и сегментов развития ОМТИ;
- предложения по партнерской и отраслевой сертификации средств автоматической (объективной) полимодельной оценке агрегированных показателей качества, конкурентной способности и перспективности развития объектов сравнительного анализа;
- предложения по сертификации качества и ранжированию лучших продуктов и услуг по автоматизации КМО и ОМТИ в целом, лидеров отраслевого, национального и мирового рынка.

Обоснована целесообразность и практическая возможность реализации названных предложений, причем, в достаточно обозримые временные сроки и при допустимых ресурсных границах.

При этом, показано, что методически и технологически обеспеченный учет и анализ системных особенностей и факторов развития ОМТИ позволяет обоснованно, консолидированно и информационно прозрачно выбирать лучшую из представляемых вариантных альтернатив развития. Тем самым, практически решать задачу оптимизации элементов и ОМТИ в целом, как для отдельных предприятий, концернов и организаций других форм собственности, так и для участников рынка в целом.

Можно утверждать, что сегодня могут быть созданы качественно новые условия и новый альтернативный вариант для цивилизованного управления рынком, характеризующийся, как бы это не было удивительным, информационной прозрачностью для участников рынка. Востребованность таких условий, как известно, характерна для национального рынка и России в целом, в первую очередь, для таких наукоемких и ресурсоемких отраслей, как кораблестроение и судостроение. Тем более, с учетом хаотической и деструктивной, практически разрушительной смены парадигм и условий мирового рынка.

Показано, что одним из вариантов использования методологии ОМКАР и его технологии реализации может быть их использование в качестве доказательной, количественно обоснованной базы формирования программ развития, а также научно обоснованных (цивилизованных) доказательств бесперспективности нерезультативных и ошибочных решений, а, тем более, макрорешений. Наконец, для формирования и ранжирования по критерию агрегированного показателя проектного качества и эффективности принятых ранее и перспективных для развития частных и комплексных управленческих решений, а также макрорешений развития КМО и ОМТИ в целом.

Алексеев А.В., Согонов С.А., Равин А.А., Хруцкий О.В., Мусатенко Р.И., Потехин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, Военный учебно-научный центр ВМФ «Военно-морская академия», Санкт-Петербургский университет МВД России

МЕТОД ОЦЕНКИ КОМПЕТЕНТНОСТИ И ПОДГОТОВЛЕННОСТИ ЭКИПАЖА СУДНА

Позитивные и негативные профессиональные качества человека, как элемента человеко-машинной (эргатической) системы должны учитываться при проектировании его деятельности на объектах управления морской техники и морской инфраструктуры (ОМТИ), особенно бортовых.

Недооценка этих качеств (человеческого фактора (ЧФ)) как отдельных членов экипажа, так и экипажа в целом приводит, как показывает печальная практика морских катастроф, к тяжелым и необратимым потерям. Связано это с тем, что, будучи составным элементом эргатической системы, человек выполняет функции приёмника, источника или преобразователя информации, вырабатывает управляющие команды и является исполнителем команд, осуществляет контроль и принимает решения. При этом на отдельных этапах, он работает как индивидуально, так и в группе, что влияет на конечный результат управления объектом и что необходимо учитывать при проектировании деятельности человека и группы с учётом регидности. Однако, если задача моделирования поведения оператора (операторов) и их ЧФ в процессе управления объектом представляется методически весьма проблематичной даже в условиях революционного совершенствования информационных технологий (в силу трудности формализации), то задача автоматической квалиметрической оценки их профессиональной компетентности и подготовленности, в том числе в составе экипажа, не только назрела, но и может быть успешно решена.

При этом понятие профессиональной компетентности (от лат. competere — соответствовать, подходить) сегодня понимается, как обобщенная мера личностной способности успешно действовать

на основе полученных в процессе обучения знаний, умений, навыков и практического опыта при решении поставленных задач.

В этом контексте профессиональная компетентность оператора объекта (далее специалиста) должна отражать обобщенный (интегральный) уровень развития личности, связанный с качественным освоением содержания образования (подготовки, переподготовки). Этот уровень проявляется в соответствии требованиям и нормам подготовки выпускника (бакалавра, магистра, специалиста) образовательного учреждения и является результатом его подготовки в рамках используемого компетентностного подхода.

Однако, общепризнанных методик обобщенной оценки личностной способности успешно действовать на основе полученных знаний, умений, навыков и практического опыта по соответствующему агрегированному показателю качества (индексу компетентности) практически нет, а в практике обучения и подготовки морских специалистов используются частные и, как правило, упрощенные методы и средства оценивания. Это, естественно, приводит к соответствующим погрешностям, а в ряде случаев, даже, к дискредитации самой необходимости квалиметрического оценивания с получением соответствующих количественных оценок.

Показана целесообразность и перспективность решения задачи оценки индекса компетентности специалиста на основе активно развивающихся в последнее время технологий автоматического квалиметрического оценивания по частным, групповым, модельным и агрегированному показателям компетентности (качества) специалиста и его подготовленности с учетом фактического состояния его компетентности и состояния готовности его заведования. Еще более значимой является оценка компетентности и подготовленности групп специалистов, экипажа корабля, судна, пароходства и т.д.

В качестве основы предложенной модели оценки индекса компетентности морского специалиста использованы: принцип системной целостности частных (учитывают многообразие специфических особенностей), групповых (учитывают специфические групповые свойства), модельных (учитывают модельное многообразие) и агрегированного показателя качества специалиста (обеспечивает системную целостность в условиях полимодельного оценивания); гармонический алгоритм агрегирования показателей, обеспечивающий минимальную методическую погрешность оценивания; технология открытого программирования Системы поддержки принятия решения и управления (СПРУ) при оценке и мониторинге компетентности и подготовленности специалиста, их групп и экипажа в целом.

Приведенные конкретные примеры реализации предложенного метода и практические оценки показали возможность и перспективность многокритериального оценивания компетентности и подготовленности специалистов при решении целого комплекса прикладных задач от планирования и прогнозирования развития персонала, обоснованного распределения ресурсов между подразделениями до оптимизации системных, архитектурных, функциональных, алгоритмических и технологических характеристик и параметров морских объектов в целом с учетом качества обслуживающего персонала.

Обоснована возможность учета индексов компетентности специалиста, персонала судна и пароходства в целом, в том числе в процессе проектирования систем автоматизации современных сложных объектов морской техники в интересах минимизации влияния человеческого фактора, прежде всего, управленческого персонала при обеспечении безопасности мореплавания.

Предложенные методология, методика и рассмотренные примеры их реализации позволяют внести в практику подготовки, аттестации, распределения и переподготовки кадров совершенно новое содержание. При этом в условиях качественно новой по уровню информационной прозрачности технологии квалиметрического оценивания (измерения) уровня знаний, практических навыков, опыта и психофизиологических особенностей специалиста обеспечивается возможность открытого, публичного и достаточно объективного конкурирования специалистов, мотивирования их на целенаправленное саморазвитие и профессиональный рост. Более того, как можно полагать, обеспечивается качественно новый уровень адекватного распределения специалистов по должностям и их использование в соответствии с предназначением и максимальной результативностью.

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, ГУМРФ имени адм. С.О. Макарова

ПРИНЦИПЫ И ЭТАПЫ ЭРГОНОМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОЕКТИРОВАНИЯ АРМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ

Эффективность функционирования системы эргономического обеспечения проектирования (ЭОП) АРМ в защищенном исполнении для специальных объектов ВМФ может быть обеспечена, если будет базироваться на ряде принципов, определяющих мероприятия по реализации ЭОП:

Первый принцип требует распределения проектных задач, которые обеспечивает ЭОП, по отдельным временным отрезкам их решения в ходе всех этапов проектирования, предусмотренных ЕСКД. Реализация этого принципа позволяет обосновать цели и взаимосвязь мероприятий ЭОП, а также степень их автономности, совокупность включаемых в них подзадач (отдельных процедур), необходимый объем информации, обеспечивающей связь между мероприятиями ЭОП.

Второй принцип - это принцип последовательности задач ЭОП. Реализация этого принципа предусматривает строгую последовательность выполнения задач (подзадач, процедур) ЭОП и своевременную выдачу информации о ходе и качестве их выполнения, т.е. о результатах эргономической экспертизы реализованных эргономических проектных решений.

Третий принцип - принцип цикличности, который предусматривает наличие многошаговых процедур ЭОП, в том числе и циклов, на всех этапах в интересах последовательной отработки структуры и содержания будущей деятельности пользователя АРМ, а также обеспечивающих ее средств и условий.

Четвертый принцип требует привлечения к решению задач ЭОП различных специалистов: конструкторов, специалистов по эргономике, дизайнеров, опытных пользователей, представителей заказчика, системных программистов, специалистов по разработке пользовательских интерфейсов, а также специалистов по тренажу, написанию инструкций по эксплуатации функциональных подсистем (ФП), для которой предназначен проектируемый АРМ.

Пятый принцип требует выбора количественных и качественных критериев и показателей для оценки уровня удовлетворения АРМ, установленным общим эргономическим требованиям (ОЭТ) на всех этапах реализации задач (подзадач, процедур) ЭОП, т.е. для проведения эргономической экспертизы.

Шестой принцип позволяет определить последовательность реализации основных функций ЭОП с учетом их взаимосвязи:

Первая функция - выбор и обоснование комплекса ОЭТ, предъявляемых ко всем объектам ЭОП, входящих в проектируемый АРМ. Эта же функция включает исходные данные для проведения эргономической экспертизы.

Вторая функция - реализация требований, установленных ГОСТ и другими нормативно-техническими документами ОЭТ в ходе ЭОП.

Третья функция - эргономическая экспертиза опытного образца АРМ на предварительных и государственных испытаниях, по результатам которой оценивается общий эргономический облик АРМ и вырабатываются, рекомендации по корректуре ряда ОЭТ и принятых эргономических решений.

Сформулированные принципы позволяют:

– четко определить функции заказчика и разработчика АРМ в ходе решения задач ЭОП и условия их взаимодействия;

– принимать и реализовывать в более короткие сроки эргономические решения в ходе проектирования АРМ с высоким качеством;

– конкретизировать задачи группы специалистов (по эргономике, дизайну, обитаемости), осуществляющих ЭОП под руководством главного конструктора проекта АРМ.

ЭОП относится к классу организационно-технических систем, специфика формирования которых состоит в создании самой системы и методов ее функционирования, а также механизмов достижения целей ЭОП эргономического облика АРМ. При формировании ЭОП, в первую очередь, необходимо определить ее целевую направленность и обосновать набор правил, определяющих форму распределения задач и полномочий между участниками проектирования АРМ, а также методы и средства принятия и реализации ими проектных эргономических решений в интересах достижения стоящих перед ЭОП целей.

ЭОП АРМ может быть реализовано в ходе трех основных этапов:

Первый этап совпадает со стадией технического предложения. Заказчиком должны быть заданы ОЭТ к проектируемому АРМ, а также роль пользователя, который будет работать на АРМ, его основные функции (задачи деятельности), его квалификация. Следует задавать требования к уровню проявления эргономических свойств и выдавать разработчику имеющиеся в распоряжении заказчика эргономические данные и предложения по организации деятельности пользователя АРМ в рабочем положении сидя.

Второй этап, совпадающий со стадией эскизного проектирования АРМ, включает трансформацию разработчиком ОЭТ (заданы заказчиком на первом этапе) в эргономический облик АРМ в целом или к его часть (элемент). На этом основании разработчик должен выдвинуть для АРМ в целом и его частям необходимые совокупности конкурирующих эргономических решений с помощью библиотеки типовых эргономических решений (ТЭР). Основная задача заказчика - сопровождение эскизного проекта с обязательной его эргономической экспертизой (на основе программы эргономической экспертизы).

Третий этап, начинающийся с технического проектирования и заканчивающийся после завершения всех видов испытаний, должен включать разработку всех конструктивных и

функциональных элементов АРМ, каждый из которых должен удовлетворять установленным ОЭТ. На этом этапе должна проводиться эргономическая экспертиза опытного образца АРМ и эксплуатационной документации, а также разрабатываться требуемые документы по ее итогам.

Все сказанное выше о ЭОП позволяет отнести ее к классу материальных, динамических, стохастических по внешним воздействиям систем организационно-технического типа. Морфологические свойства ЭОП в основном зависят от состава возлагаемых на нее функций и взаимосвязей между ними. Особенно следует подчеркнуть роль обратных связей, работающих в ходе эргономической экспертизы принципиальных проектных эргономических решений. По характеру связей ЭОП можно отнести к многосвязным, иерархическим системам, а по структуре - к системам детерминированным. ЭОП является рефлексивной системой, т.е. она способна генерировать информацию как о необходимости введения новых ОЭТ, так и о расширении номенклатуры ТЭР при создании новых типов АРМ.

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, ГУМРФ имени адм. С.О. Макарова

ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЛИКА ИНТЕГРИРОВАННОЙ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ

Основываясь на структуре и функциях территориальных подразделений ВМФ, можно утверждать, что принципиально важным для проектирования интегрированной АСУ специальных объектов ВМФ в защищенном исполнении является наличие следующих видов ее описания:

1. Цели деятельности специальных объектов ВМФ.
2. Задачи, решаемые территориальными подразделениями ВМФ.
3. Процессы управления, реализуемые органами управления ВМФ.
4. Функции управления, выполняемые лицом, принимающим решение (ЛПР), и составом их органов управления в процессе управления подразделениями ВМФ.
5. Стандарты и протоколы, регламентирующие обработку информации и обмен ею в рамках корпоративной сети.
6. Информационные ресурсы, необходимые для осуществления процессов и функций управления.
7. Информационные технологии (ИТ), используемые ЛПР и их органами управления.
8. Прикладные платформы, реализующие обработку информации.

При этом процессы управления строятся относительно специальных объектов ВМФ, а функции управления, выполняемые персоналом в ходе реализации процессов управления, должны быть обеспечены соответствующим информационным ресурсом (ИР), характеризующим какую-то одну сторону объекта управления.

Перечисленные виды описаний должны использоваться проектировщиком для решения следующих задач:

1. придание проектируемой интегрированной АСУ требуемых заказчику ВМФ потребительских свойств с точки зрения практических задач управления подразделениями ВМФ и подчиненными им учреждениями;
2. встраивание интегрированной АСУ в действующую систему управления ВМФ и ее интеграция с взаимодействующими системами управления администрации субъекта федерации;
3. оценка состава и качества применяемых информационных технологий;
4. оценка достаточности планируемых к обработке и хранению ИР, исходя из номенклатуры автоматизируемых функций управления (АФУ), выполняемых интегрированной АСУ;
5. оценка форматов потребляемых, производимых и хранимых ИР;
6. разработка предложений по рациональной визуализации ИР в интересах ЛПР и пользователей;
7. минимизация избыточности ИР;
8. полноценное использование действующих телекоммуникационных систем;
9. сокращение стоимости создания ИАСУ за счет унификации аппаратно-программного оборудования АРМ, информационных технологий и прикладных платформ.

Совокупность проектных решений, принятых при решении перечисленных задач, определяет целостный облик проектируемой АСУ, состоящий из технического, экономического, информационного и эргономического обликов. Технологии разработки технического и экономического обликов АСУ разработаны и широко применяются. Поэтому возникает задача разработки информационного облика проектируемой интегрированной АСУ ВМФ на принципах общего информационного ресурса (ОИР), реализуемого в рамках компьютерной сети (КС).

Исходя из номенклатуры решаемых информационных задач, следует под информационным обликом интегрированной АСУ ВМФ считать совокупность описаний и конструкторских решений по:

1. перечню решаемых управленческих задач и номенклатуре автоматизируемых процессов и функций управления;

2. составу и формам использования, воспроизводства и хранения ИР;

3. составу ИТ и прикладных платформ.

Основное назначение информационного облика интегрированной АСУ ВМФ состоит, во-первых, в идентификации функций, функционального окружения и информационных потребностей пользователей. Во-вторых, в идентификации стандартов, соглашений и правил взаимодействия как внутренних компонент проектируемой интегрированной АСУ, так и ее взаимодействия с внешними системами (МО РФ, администрация субъекта федерации). В-третьих, в идентификации прикладных платформ, необходимых для обеспечения функционирования интегрированной АСУ ВМФ.

При формировании информационного облика интегрированной АСУ целесообразно использовать понятие функциональной подсистемы (блока) – как совокупности ИР и ИТ, ориентированных на определенную прикладную платформу и обеспечивающей реализацию функций управления. Следует также разделять ИТ на специализированные, учитывающие специфику конкретной предметной области (управление отделами, центрами и др. подразделениями ВМФ), и базовые. Под базовой платформой комплекса средств автоматизации (КСА) следует понимать структурированный набор ИТ и стандартов, средств их реализации, обеспечивающий деятельность подразделений ВМФ.

Формирование информационного облика интегрированной АСУ ВМФ должно осуществляться с использованием ряда концептуальных моделей:

1. Модели примерной структуры специальных объектов ВМФ.

2. Модели информационного облика ИР специальных объектов ВМФ.

3. Модели процесса управления подразделениями ВМФ и подчиненными им учреждениями (должна специально разрабатываться на основе номенклатуры выполняемых функций управления в каждом органе управления).

4. Модели цикла управления.

5. Модели функций управления, определяемые на множестве ИР и вырабатываемые для управления свойствами и состояниями объекта управления, его задачами и действиями и выработкой собственно управляющих воздействий.

Информационный облик интегрированной АСУ ВМФ должен разрабатываться с учетом трех уровней представления:

1. функционального, определяющего информационные функции системы, которые должны удовлетворять потребности пользователей КС ВМФ;

2. системного, определяющего совместимость и взаимодействие компонент интегрированной АСУ как между собой (внутри системы), так и с внешними системами (МО РФ, администрация субъекта федерации);

3. технического, определяющего структуру и основные свойства технических средств интегрированной АСУ.

При синтезе КСА органа управления должна разрабатываться:

- функционально-техническая модель КСА, содержащая описание типовых функциональных компонент;
- комплекс моделей видов обеспечения КСА, включающий модель аппаратных средств, программного и информационно-лингвистического обеспечения;
- модели протоколов и служб КСА.

Можно предположить, что применение унифицированных методов структурного анализа и CASE – технологий при синтезе интегрированной АСУ специальных объекта ВМФ внесет новый вклад в качество и снижение трудоемкости и стоимости проектирования.

Баркова Н.А., Грищенко Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИОННОЙ ДИАГНОСТИКИ ПЛАНЕТАРНЫХ РЕДУКТОРОВ НА МОРСКОМ ТРАНСПОРТЕ

Ограниченные по габаритам планетарные редукторы широко используются на морском транспорте в составе мощных гребных установок, электрогенераторов с газотурбинным приводом и других судовых механизмов. В то же время их эксплуатационная диагностика, в отличие от диагностики других составных частей энергетических установок, не получила широкого развития из-за сложности обнаружения дефектов наиболее нагруженных элементов редуктора – подшипников сателлитов.

В докладе приводятся результаты исследований вибрации трех групп двухступенчатых и трехступенчатых планетарных редукторов. Каждый редуктор имеет ступени с вращающейся и

неподвижной коронами. Основная задача исследований – поиск признаков дефектов, в первую очередь износа наиболее нагруженных подшипников сателлитов.

Первая из решенных задач – определение списка частот основных составляющих вибрации каждой ступени планетарного редуктора, ее осевых подшипников и подшипников сателлитов, отвечающих за появление возможных дефектов, а также выражений для их расчета.

Вторая – анализ изменений уровней этих составляющих вибрации во времени и по группе одинаковых редукторов, в результате которого установлены основные причины роста наиболее сильных составляющих каждой ступени планетарного редуктора, кратных частотам вращения ее узлов и зубцовым частотам. В качестве основной причины роста зубцовых составляющих вибрации, вибрации на частоте вращения промежуточной ступени и на четных гармониках частоты вращения короны и/или сателлитов определен износ одного из подшипников сателлитов.

Третья – оценка возможности выделения высокочастотной вибрации, возбуждаемой конкретным подшипником, жестко закрепленным в корпусе многоступенчатого планетарного редуктора. Экспериментально установлена возможность идентификации дефектного подшипника из всех, используемых в сателлитах одной ступени редуктора с неподвижным водилом. В большой группе трехступенчатых редукторов обнаружен один с дефектом подшипника качения выходного вала с частотой вращения в 160 раз ниже частоты вращения входного вала, т.е. при соотношении вклада низкооборотного подшипника в вибрацию редуктора не более 1/10000.

По результатам исследований разработан модуль диагностики конкретного типа планетарного редуктора для стационарной системы контроля и диагностики электрогенерирующей установки с газотурбинным двигателем. Система диагностики введена в действие в начале 2015 года.

Белячков С.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

УГРОЗЫ "ИНТЕРНЕТА ВЕЩЕЙ»

Производители электроники все чаще стремятся наделять «разумом» предметы, называя это Интернетом вещей (Internet of Things, IoT). Частью Интернета вещей является широкий спектр кухонной электроники (кофеварки, холодильники, микроволновые печи), домашней развлекательной техники (Smart-телевизоры, музыкальные центры), систем домашней безопасности и многие другие устройства.

Сегодня в мире к сети подключено от 6 до 14 млрд. автономных «умных» устройств, оснащенных различными датчиками, не учитывая смартфоны, планшеты, персональные компьютеры и ноутбуки. А к 2020 году, по мнению экспертов, количество подключенных устройств составит более 26 млрд.

Однако все эти устройства могут быть потенциальным источником угрозы. Не зря аббревиатуру IoT нередко расшифровывают как “Internet of Threats”, т.е. “Интернет угроз”.

Для обеспечения достаточной защищенности умной электроники зачастую требуются высокий уровень знаний в областях шифрования и администрирования, что недоступно для «рядовых» пользователей. Зачастую безопасность устройств обеспечивается только в рамках протоколов коммуникации (например, настройки безопасности WiFi).

Поэтому для злоумышленника не составляет особого труда внедрить вредоносное программное обеспечение (ВПО) и использовать потребительские устройства для нарушения информационной безопасности их владельцев:

1. Использование умных устройств для проникновения на персональные компьютеры и мобильные телефоны. Интернет вещей позволяет устройствам получить доступ к домашней или офисной локальной сети. Так как домашняя сеть воспринимается персональными компьютерами и мобильными телефонами в качестве доверенной, то они не имеют возможности защититься от атаки с умных устройств.

2. Использование умных устройств для создания ботнетов. Подключение устройств к сети Интернет позволяет злоумышленникам использовать умные устройства во многих интернет-активностях от DDoS-атак и рассылки спама до вирусных эпидемий.

3. Слежка за пользователями. Не секрет, что умная электроника, тайно или явно, отправляет своим производителям различные данные: режим дня, вкусовые предпочтения, записи разговоров, местоположение и т.д. Вся эта информация, попав не в те руки, может привести к последствиям разной степени серьезности: от трагетированной рассылки спама до шпионажа.

В более серьезных случаях захват устройства может привести к человеческим жертвам, например, в случае дистанционного перехвата управления автомобилем.

Основной проблемой обеспечения безопасности устройств, связанных с Интернетом вещей, является нежелание производителя поддерживать устаревшее устройство. Современные тенденции показывают, что сегодня даже на смартфон двухлетней давности, как правило, уже невозможно

поставить современную версию операционной системы. Цифровые продукты «обречены» доживать свой короткий век без исправлений и «заплаток». С теми уязвимостями, которые в них обнаружились.

Чтобы обеспечить безопасность устройств, подключенных к IoT, необходимы усилия всех участников рынка. Не секрет, что большую часть «Интернет-вещей» производят небольшие стартапы, существующие менее 3-х лет и, которые, зачастую, не могут себе позволить содержать армию экспертов по безопасности, вовремя предотвращать взломы.

Поэтому им приходится рассчитывать только на уровни защиты аппаратного и программного обеспечения, приобретенного у поставщиков, из-за ценовой политики которых не все производители могут купить хорошо защищенные компоненты.

Также необходимо развивать обучение, как пользователей, так и производителей. Далеко не все пользователи понимают, какие угрозы таят в себе с виду безопасные приборы. Они не обладают достаточными знаниями для самостоятельной настройки даже простейших средств обеспечения безопасности устройства.

А начинающим производителям будет не лишним узнать, что вопросы безопасности должны быть первоочередными на всех этапах IoT-проекта — от идеи до серийного выпуска. И, даже, после и во время эксплуатации. Они не могут получить доступ к передовому оборудованию и сделать свой вклад в развитие систем безопасности.

В докладе предложены к обсуждению как уязвимости и угрозы «Интернета вещей», так и пути информационного противодействия им.

Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Согонов С.А., Ушакова Н.П., Петров А.А., Кузьмина С.Д., Поленин В.И., Соловьев С.Н., Москаленко В.А., Мусатенко Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, Санкт-Петербургский государственный морской технический университет, АО «Концерн «НПО «Аврора», Центральный научно-исследовательский и проектно-конструкторский институт морского флота, Институт проблем управления РАН, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: ВТОРОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ

Систематизация данных и знаний для таких предметных областей, как автоматизация процессов борьбы за живучесть корабля, судна, имеет исключительно большое значение. Это обусловлено особой востребованностью научных знаний по всем аспектам данной большой проблемы, теории и практики разрешения проблемных вопросов, возникающих в предметной области и в «пограничных» областях теории и практики борьбы за живучесть корабля, судна. Более того, определенной ведомственной разобщенностью специалистов, создающих и развивающих новые информационные технологии и высокотехнологичные решения в данной комплексной предметной области.

В этой связи по инициативе ряда ведущих предприятий и учебных заведений в ОАО «Концерн «НПО «Аврора» 6 декабря 2012 г. в обеспечение комплекса работ по созданию систем автоматизации управления боевыми кораблями и подводными лодками ВМФ была проведена специализированная Первая научно-практическая конференция «Современные технологии автоматизации процессов борьбы за живучесть (АПБЖ-2012)». По итогам конференции возникла идея написания открытой коллективной монографии по теме «Автоматизация процессов борьбы за живучесть корабля, судна».

Особая актуальность этой темы обусловлена, с одной стороны, интенсивным развитием теории и практики борьбы за живучесть корабля, судна (БЖКС), соответствующих технологий автоматизации процессов БЖКС, а, с другой стороны, их востребованностью на всех этапах жизненного цикла создания и эксплуатации кораблей, судов.

Важнейшей целью создания коллективной монографии явилось способствование развертыванию в широком кругу специалистов дискуссии и обмена опытом для разрешения возникающих проблем создания и эксплуатации современной техники, которая сегодня представляет собой большие и структурно сложные системы. Более того, для системного осмысления открывающихся новых широких возможностей современных информационных технологий, взвешенного оценивания качественно новых возможностей, роли и специфических особенностей главного элемента системы автоматизации – операторов. В первую очередь – в лице командиров кораблей и подводных лодок, капитанов судов, включая, безусловно, как позитивные, так и специфические негативные их свойства, обусловленные так называемым «человеческим фактором».

Для достижения этой цели впоследствии были организованы и проводятся аналогичные специализированные конференции по проблеме автоматизации процессов борьбы за живучесть корабля, судна (АП БЖКС), а также специализированный Цикл научно-практических семинаров, в том числе в форме мастер-классов, по обобщению лучших практик в этой области. В результате был накоплен значительный объем научных и практических данных с их отражением в монографии.

Реализация данной миссии и организация мероприятий были возложены на специально созданное в 2012 г. Некоммерческое партнерство «Институт автоматизации процессов борьбы за живучесть корабля, судна (ИАП БЖКС)».

Как итог, в 2015 г. была завершена работа по созданию Первой электронной версии монографии «Автоматизация процессов борьбы за живучесть корабля, судна» с ее представлением на Третьей конференции АП БЖКС (см. Материалы «ИБРР-2015», с. 253).

В текущем году на этой базе была продолжена работа по систематизации, классификации и актуализации накопленных данных и знаний по рассматриваемой проблеме, включая вопросы теоретического обоснования, анализа, синтеза и оптимизации процессов АП БЖКС, обобщения и обоснования практик создания, построения, освоения и эксплуатации перспективных средств обеспечения безопасной эксплуатации и локализации аварийных ситуаций в части обеспечения непотопляемости, взрыво-пожаро- и радиационной безопасности корабля, судна; живучести технических средств и оружия, защищенности экипажей кораблей, судов и управляемости (качества) системы автоматизированного управления БЖКС.

Во Второй электронной версии коллективной монографии «АП БЖКС» нашли отражение обобщения и ранжирования лучших практик обеспечения БЖКС, оценки конкурентной способности в интересах ускоренного практического освоения (инновационного обеспечения) лучших проектных и управленческих решений. Прикладная направленность представляемой коллективом авторов монографии обусловлена в этой связи необходимостью формирования коллективного мнения практиков – ведущих специалистов данной предметной области в части вопросов истории развития проблемы, анализа публикаций в России и за рубежом, методологии исследования, ранговой партнерской сертификация средств и систем АП БЖКС и аттестации объектов автоматизации в целом.

В докладе обсуждаются наиболее значимые и проблемные вопросы, вошедшие во Вторую электронную версию коллективной монографии, а также наиболее важные методологические вопросы и результаты с целью дальнейшего коллективного осмысления полученных теоретических и практических знаний по данной большой и сложной проблеме.

Бронников А.А
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ ТЕХНОЛОГИИ ШИФРОВАНИЯ WEP ДЛЯ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ

Технологии беспроводных сетей сегодня являются одними из самых популярных и востребованных в мире. Они повсеместно вошли в нашу жизнь. Многие пользователи уже не могут представить свой день без смартфона с постоянным выходом в Интернет. В связи с этим остается остро востребованным вопрос о необходимости защиты данных пользователей.

Одна из самых популярных технологий беспроводных сетей в настоящее время – сети Wi-Fi (Wireless Fidelity), которые основываются на стандарте IEEE (Institute of Electrical and Electronics) 802.11. Для защиты информации в сетях Wi-Fi в настоящее время широко используется алгоритм безопасности Wired Equivalent Privacy (WEP), являющийся базовым средством обеспечения безопасности при аутентификации, идентификации пользователя, а также шифровании передаваемого трафика.

Алгоритм безопасности WEP, как известно, основан на поточном шифре RC4, который сочетает в себе высокое быстродействие и возможность использования переменной длины ключа. Размер ключа 64 или 128 бит, его статическая составляющая варьируется от 40 до 104 бит, а вектор инициализации равен 24 бит. Вычисление контрольных сумм осуществляется алгоритмом CRC32. Шифрование данных производится операцией XOR с псевдослучайной ключевой последовательностью.

Но протокол WEP, как известно, имеет немало уязвимостей и не является гарантией полной сохранности и безопасности данных. Один из главных недостатков этого алгоритма безопасности – это статический ключ.

Методы взлома WEP можно условно разделить на два вида:

1. Пассивные сетевые атаки – ключ шифрования вычисляется с помощью фреймов, пассивно собранных в беспроводной локальной сети. Данный метод был установлен криптоаналитиками С. Флурером, И. Мантином и А.Шамиром.
2. Активные сетевые атаки - повторное использованием вектора инициализации (IV Replay) и манипуляция битами (Bit-Flipping).

В частности, взлом WEP способен осуществить любой подготовленный пользователь, имеющий доступ в интернет. Для этого достаточно всего лишь несколько утилит (к примеру, BackTrack Live CD) и 15 минут времени. В докладе продемонстрирован один из векторов атаки на беспроводные сети с технологией WEP.

Подробно рассмотрены и проанализированы способы повышения защиты WEP:

Фильтрация MAC адресов беспроводных адаптеров клиентов сети.

Hide SSID – скрытие идентификатора SSID беспроводной сети.

Dynamic WEP – использование динамических ключей при передаче.

WEP Plus – избегание слабых векторов инициализации.

Показано, что в настоящее время, протокол WEP является малоэффективным и несовершенным средством защиты беспроводной сети. Рекомендуется переходить на более совершенные алгоритмы обеспечения безопасности типа WPA и WPA2.

Гоманцов А.А., Горбачев В.А.
Россия, Санкт-Петербург, АО Центральное конструкторское бюро морской техники «Рубин», Военно-морской политехнический институт, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

К ВОПРОСУ О СИСТЕМНОЙ БЕЗОПАСНОСТИ СУДОВЫХ ЭНЕРГЕТИЧЕСКИХ КОМПЛЕКСОВ

Опыт использования сложных судовых энергетических комплексов указывает на значительный уровень аварийности в различных условиях эксплуатации. Несмотря на применяемые меры организационного и технического характера, проблема предупреждения аварийности судовой техники продолжает оставаться актуальной.

В общем объёме задач особое место занимают такие, которые позволяют выделить и проанализировать влияние классов начальных состояний на динамику развития аварии, в том числе с учетом эксплуатационных факторов. Способность судна и его технических средств к устойчивости и сохранению работоспособности при появлении отказов или повреждений является важным системным показателем.

Рассмотренная в статье задача прогнозирования появления отказов или повреждений с помощью математической модели с распространённым лагом и алгоритма классификации по выделению классов в пространстве, а также критериев учета рисков позволяет принимать меры по предотвращению возникновения аварийных ситуаций, и существенно продлить службу судовых энергетических комплексов.

Для рассмотрения поставленной задачи введём некоторые понятия и определения в системе безопасности кораблей.

Отсутствие нормативных определений позволяет сформировать и выделить некоторые из них в порядке научного обсуждения.

Системной безопасностью будем называть совокупность взаимодействующих объектов, функционирование которых описывается набором эксплуатационных показателей (параметрической базой), и набором алгоритмов локализации.

Такое определение придаёт понятию системной безопасности более узкий смысл и вводится для удобства использование некоторых терминов из теории управления.

Всё то, что не входит в систему, будет образовывать внешнюю среду по отношению к ней, а воздействие внешней среды осуществляется через экзогенные (внешние) переменные, а эндогенные (внутренние) переменные определяются самой системой. Таким образом, любая модель определяется эндогенными переменными через внешние (экзогенные) факторы.

Так же было введено понятие кусочно-постоянной динамической модели развития аварии (отказа) на основе учета влияния причинно-следственных связей в виде опорного множества классов начальных состояний и для выработки соответствующих векторов управления локализации. Подобное концептуальное определение основано на анализе ковариационной матрицы, отражающей линейный тренд изменения аварийности в зависимости от темпов развития вооружения и технических средств и уровня автоматизации.

Для рассмотрения математической модели была сформулирована задача и возможные способы ее решения: в многомерном пространстве состояний системы безопасности необходимо разделить (классифицировать) эксплуатационные показатели в виде нормальных (случайных) величин, которые обладают одинаковыми средними значениями, но отличаются по дисперсии хотя бы в одном каком-то направлении.

В большинстве практических случаев точки смешанной выборки разделены в пространстве признаков равномерно по всему объёму. Такое условие позволяет для классификационной матрицы ввести допущение, чтобы её собственные члены были равны дисперсии точек выборки линейного тренда колебаний уровня аварийности (объема отказов) осреднённых по всем кораблям данного соединения.

При решении прикладных задач такого рода количество критериев увеличивается за счет отдельного рассмотрения трудноизмеримых компонентов ущерба (материальные затраты, человеческие потери, экологический ущерб и т.д.).

В случае возникновения трудностей, связанных с вычислением величины ущерба (или его отдельных компонентов), рассматриваются показатели, косвенно связанные с величиной возможного ущерба.

Горбенко Е.А., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ МЕР ПО ПРЕДОТВРАЩЕНИЮ ИСПОЛЬЗОВАНИЯ SQL-ИНЪЕКЦИЙ В ИНФОРМАЦИОННЫХ РЕСУРСАХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Базы данных (БД) являются одним из самых удобных инструментов для работы с информацией. Они широко используются в различных web-приложениях и продуктах программного обеспечения (ПО). В БД может храниться информация любого рода: от финансовой информации пользователей до личных данных сотрудников. Данный факт говорит о безусловной необходимости защиты баз данных от несанкционированного доступа.

Одной из самых распространенных форм атак на БД является SQL-инъекция ─ атака, в ходе которой модифицируется запрос к базе данных, изменяющий логику его выполнения так, как это необходимо злоумышленнику. В некоторых случаях SQL-инъекция позволяет писать/читать файловую систему с правами сервера баз данных. Уязвимость возникает в большинстве случаев из-за недостаточной фильтрации данных при построении запроса.

Обычно SQL-инъекции рассматривают как атаку на web-приложения. На самом деле в зоне риска оказываются и клиент-серверные, и сервис-ориентированные приложения, использующие системы управления базами данных (СУБД). Согласно отчету «Уязвимости веб-приложений» компании Positive Technologies (2016) критически опасная уязвимость «Внедрение операторов SQL» (SQL-Injection) вновь вошла в топ-10 самых опасных уязвимостей.

Таким образом, существует необходимость обратить внимание на методы предотвращения реализации данной атаки, в том числе на объектах морской техники и морской инфраструктуры (ОМТИ), для которых характерны соответствующие специфические уязвимости и угрозы.

К последствиям внедрения SQL-инъекций относят:

- появление у злоумышленника дампа (снимка или копии) базы данных;
- раскрытие системной информации о состоянии БД;
- нарушение доступности, целостности и/или конфиденциальности информации БД;
- внедрение backdoor (тайный доступ к данным);

Профилактические средства против возможности внедрения SQL-инъекции в базу данных достаточно просты в реализации, но часто игнорируются администраторами БД. Это дает злоумышленникам возможность несанкционированного доступа к информации. К наиболее эффективным мерам предупреждения SQL-инъекций относят:

- сведение к минимуму числа динамических запросов;
- проверка ввода данных;
- своевременная установка обновлений ПО СУБД;
- минимизация количества неиспользуемого функционала;
- использование автоматизированных средств защиты от SQL-инъекций;
- регулярный мониторинг логов СУБД на ошибки;
- правильная конфигурация работы СУБД;

Следует заметить, что устойчивость БД к SQL-инъекциям во многом зависит от администратора БД, что лишний раз подтверждает зависимость информационной безопасности от «человеческого фактора». В докладе подробно рассмотрены средства предотвращения внедрения SQL- кода и оценена эффективность работы каждого из них, подробно рассмотрены автоматизированные средства защиты от SQL-инъекций.

Перспективность данного метода обусловлена сегодня наличием средств автоматического внедрения SQL-инъекций типа jSQL Injection. В настоящее время существуют также ряд программных средств обнаружения инъекций, например, расширение для Firefox «SQL Inject ME». Различные автоматизированные средства для поиска SQL-инъекций и основные принципы работы данного ПО также рассмотрены в докладе.

Таким образом, в работе приведены основные методы предотвращения атак на БД, проведен краткий анализ автоматизированных средств защиты от внедрения SQL-кода, предложен ряд рекомендаций для администраторов БД, обоснована актуальность темы применительно к ОМТИ.

Тем самым сделан вывод о необходимости сочетания мер по организации работы с БД и автоматизированных средств по защите от атак на основе SQL-инъекций в информационных ресурсах объектов морской техники и морской инфраструктуры.

Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ИЗМЕНЕНИЕ СТРАТЕГИИ УПРАВЛЕНИЯ РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ ПРЕДПРИЯТИЯ МОРСКОЙ ИНФРАСТРУКТУРЫ

В настоящее время предприятия, в том числе морской инфраструктуры, развиваются в условиях повышенной неопределенности, имея мало и трудно прогнозируемое финансовое будущее. Деятельность организаций подвержена множеству рисков, которые могут привести к банкротству. Управление рисками является основополагающей фактором стабильного развития финансовой системы предприятия в целом, а в последнее время даже выделяется, как отдельная отрасль знаний, называемая риск-менеджментом.

Сегодня риск-менеджмент в России активно развивается и стране еще предстоит решить множество задач в этом направлении. Стратегии и приемы управления организацией часто заимствуются от западных компаний и носят скорее поверхностный характер. Поэтому актуальным вопросом для российских компаний является создание и развитие национальных методик и стратегий управления, ориентированных как на финансовую политику России в целом, так и на отдельные отрасли. Не исключением является и морская отрасль, которая находится в целом на высоком уровне технологического развития. Соответственно, ей присущи большое количество разнородных рисков.

Целью риск-менеджмента является повышение вероятности возникновения и воздействия благоприятных событий и снижение вероятности возникновения и влияния неблагоприятных для организации событий в ходе ее деятельности. Управление рисками включает в себя процессы, относящиеся к планированию управления рисками, их идентификации и анализу, реагированию на риски, а также их мониторингу, для чего используется широкий спектр информационных технологий.

Каждый из рассматриваемых процессов имеет свои характерные особенности, присущие отдельным этапам развития предприятия. В общем случае принципы риск-менеджмента подвергаются изменениям на разных этапах жизненного цикла организации. На каждом из этапов: зарождение, рост, стагнация, спад возможно построение стратегии управления рисками, проработка тактики и методологии.

Первые этапы развития организации, в том числе и предприятия морской торговли, как правило, не включают в себя оценку и анализ рисков. Любые, еще не такие значительные потери относятся на счет неопределенности, свойственной рыночной экономики.

На дальнейших этапах развития объекта морской инфраструктуры, как предприятия высокого статуса, целью которого часто является выход и закрепление на международном уровне, анализу, оценке и в целом управлению рисками выделяется основное место. Определяя свое место в морской отрасли, организация прогнозирует свои успехи и выбирает выгодную для себя стратегию. Возможны два варианта исхода события: или компания начинает более активное расширение и выходит на рынок с новыми рисками, либо деятельность компании угасает и, даже, прекращается.

Детальный анализ и прогноз на каждом этапе жизненного цикла организации риска, понимание его дальнейшего поведения в рамках деятельности организации позволяет оценивать степень его изменения и возможный вектор развития.

Для расчета и оценки рисков применяются различные расчетные методы, обосновываются различные математические модели. В зависимости от сформированной стратегии компания выбирает для себя наиболее эффективную теорию и модель риска с дальнейшим ее практическим использованием для управления производственной деятельности.

Например, разрешению различных маркетинговых ситуаций служат методы теории игр для принятия решений в условиях неопределенности и риска. Ценность переменных, фигурирующих в теории игр, определяется информацией, которую они несут о конкуренте. Среди них - структура затрат конкурентов, состояние спроса, потенциал рынка. В основе теории игр лежит оценка действий конкурирующего предприятия, выбор стратегий на основе полученных данных и прогнозирование развития ситуаций.

В докладе приведены результаты анализа влияния изменения стратегии управления рисками на разных этапах жизненного цикла предприятия морской инфраструктуры и показана возможность их существенного снижения/роста от согласованности стратегий партнеров, а также возможность эффективного использования в этих условиях современных информационных сервисов и программных комплексов поддержки принятия управленческих решений.

Каганский М.А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

КРИТИЧНОСТЬ ВЛИЯНИЯ СУБЪЕКТИВНЫХ СВОЙСТВ ОПЕРАТОРОВ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ ВМФ НА КАЧЕСТВО И РЕЗУЛЬТАТЫ УПРАВЛЕНИЯ

Современный этап развития организационно-технических систем (ОТС) ВМФ характеризуется созданием единого информационного управляющего пространства (ЕИУП) путем интеграции разнородных эргатических комплексов и систем в единое целое.

ОТС ВФМ - это системы, в которых осуществляется и управление техническими средствами и управление операторами (людьми), включая лиц, обосновывающих управленческие решения (ЛОР), их принимающих (ЛПР, руководителей) и исполняющих (ЛИР).

Важнейшая функция ОТС ВМФ - это управление силами и средствами, которая понимается как целенаправленный процесс (деятельность) ЛПР (главнокомандующего, командующих, командиров, начальников штабов и других органов военного управления) по поддержанию боевой готовности сил (войск), подготовке операций (боевых действий) и организации выполнения силами (войсками) поставленных им тактических, оперативно-тактических или оперативных задач.

Техническая сложность современных организационно-технических систем управления постоянно возрастает, сокращается время на принятие решения, увеличивается количество источников информации и объемы информации. Однако, при этом часто недостаточное внимание уделяется совершенствованию процессов человеко-машинного (эрготехнического) взаимодействия, достаточно полному и адекватному учету в контуре управления субъективных свойств операторов. Это, безусловно, оказывает непосредственное негативное влияние на качество и результаты управления, защищенность циркулирующей в контуре управления информации и безопасность службы экипажей кораблей, подводных лодок, самолетов и др.

Так, например, при планировании операций и анализе результатов их проведения необходимо кроме оценки значимости вклада оружия и технических средств уметь оценивать и учитывать качество управления силами, оружием и техническими средствами, участвующими в боевых действиях. Причем, необходимо адекватно учитывать широкий спектр разнородных факторов, непосредственно влияющих на качество и результаты управления, а также многочисленных аспектов разнородных предметных и междисциплинарных областей знаний: системного анализа-синтеза, эргономики, психологии, физиологии, антропометрии, биомеханики, хронобиологи, и и др.

Под управлением силами флота в ЕИУП следует понимать непрерывный интеллектуально-информационный процесс добывания, преобразования весьма значительных объемов данных и использования информации при решении общих задач и достижения единых целей, осуществляемый командованием и штабами с широкомасштабным использованием современных средств автоматизации управления, освещения обстановки и связи.

Процесс управления, как правило, всегда инициируется ЛОР, ЛПР, а в ряде случаев и ЛИР. Это означает, что ЛПР формирует и реализует процесс управления либо относительно внешней задачи (поставленной вышестоящим начальником), либо сам формирует и реализует задачу по достижению целей действий своей системы на основе предоставленных полномочий, оценки обстановки и предназначения системы. При этом, действия ЛПР в процессе управления носят, естественно, сознательный, осмысленный характер, но подверженный в отдельных случаях возможному негативному влиянию субъективных свойств личности типа страх, меркантильность, неадекватность.

Из-за возможных последствий для боевой системы и творческого характера работы ЛПР наиболее сложным и ответственным среди них является, как известно, этап принятия решения. Решение, принятое ЛПР на каждом из этапов боевых действий, является основой управления.

Следовательно, основные составляющие процесса управления и ЕИУП — это интеллект, креативность, информация и время, а основной продукт этого процесса — решение и его адекватность фактической тактической, оперативно-тактической и оперативной ситуации. В общем случае оно может быть различным по достигаемому уровню качества - от нерезультативного, неэффективного до рационального и оптимального. Следует отметить, что практике квалиметрии решений, их метрике, априорному и апостериорному анализу и синтезу даже сегодня уделяется далеко не достаточное внимание, хотя именно качество решений является ключевым фактором результативности боевых действий, обеспечения безопасности службы личного состава.

Одной из характерных черт функциональной части ИР является наличие в ней эвристических процедур обработки информации, что также непосредственно связано с субъективными (позитивными и негативными) свойствами ЛОР, ЛПР, ЛИР. Эвристические процедуры обработки данных связаны с деятельностью конкретного оператора и зависят от его интеллектуальных возможностей, мотивации, состояния и многих других факторов.

В докладе рассмотрены особенности процесса управления ВМФ и роль ЛОР, ЛПР и ЛИР в нем. Проанализированы принципы эргономики, подходы к стратегии построения архитектуры и функционала эффективных организационно-технических систем с учетом человеческого фактора. Определены важность и современные особенности учета эргономических показателей.

Рассмотрены принципы модели SHELL, в которой центральное место при построении эргатической системы занимает человек со своим субъективным набором свойств и характеристик, соответствующих ограничений (психосоматических, когнитивных, мотивационных и др.). Выделены основные направления исследований и проблемных вопросов, связанных с влиянием субъективных свойств операторов на качество ОТС ВМФ, качество и результаты управления, границы критичности влияния, в том числе при использовании современных информационных, аналитических и интеллектуальных (когнитивных) автоматизированных систем поддержки принятия решений операторов и управления ОТС ВМФ.

Рассмотрены известные критерии и алгоритмы агрегированной полимодельной оценки «качества оператора» в контексте их ранжирования, оценки критичности и уровня соответствия (аттестации) различным должностным требованиям. Сформулирована парадигма рефлексивного управления «качеством оператора» для оптимизации структуры, свойств и характеристик ОТС ВМФ в различных режимах и модельных сценариях их использования.

Кальбфляйш В. А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ЛИЧНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОСВЕДОМЛЕННОСТЬ ОБ ОКРУЖАЮЩИХ УГРОЗАХ

В современном мире каждый человек, не зависимо от его возраста, специальности и места работы, постоянно находится в потенциально опасной среде с точки зрения угроз информационной безопасности (ИБ). Количество информационных потоков, с которыми каждый из нас взаимодействует на ежедневной основе, за последнее десятилетие выросло многократно. И при каждом взаимодействии имеется риск раскрытия как конфиденциальной информации, так и персональных данных, будь то вследствие действий злоумышленника или же из-за собственной безалаберности. Случаи, когда вместе с фото, сделанным за рабочим местом, в социальные сети попадали пароли или другая конфиденциальная информация, к сожалению, не единичны.

Многие инциденты ИБ на предприятии в своей основе имеют одну и ту же проблему – крайне низкую осведомленность сотрудников о правилах, в первую очередь, личной информационной безопасности. С целью исправить данную ситуацию и обеспечить сохранность корпоративных интересов, службы ИБ на регулярной основе проводят мероприятия по разъяснению правил безопасности. И здесь явным образом видно несоответствие, в котором, впрочем, нельзя упрекнуть сотрудников служб безопасности - их рабочими обязанностями является, в первую очередь, предотвращение финансовых потерь предприятия.

Однако, угрозы хищения или повреждения конфиденциальной информации не являются прерогативой корпоративного сектора. Они никуда не исчезают, когда мы покидаем рабочее место. Наоборот, средства массового спроса, которыми мы пользуемся в личным целях и быту, являются наиболее уязвимыми для эксплуатации злоумышленником. Существует множество векторов атак: от перехвата незащищенного трафика до установки на устройство троянской программы. И рынок мобильных устройств является золотой жилой для злоумышленника не в последнюю очередь из-за крайне низкой осведомленности рядового пользователя о опасностях, что его окружают.

Целью данного доклада является привлечение внимания к проблеме фактического отсутствия понятия «личная информационная безопасность» в умах граждан и в контексте ИБ личности, общества, государства. Необходимо начать планомерную работу по повышению осведомленности об окружающих угрозах не только с подачи служб безопасности предприятий, но и на базе ВУЗов и, даже, школ. Ведь, доступ к мобильным устройствам и интернету появляется у детей раньше, чем к публичной библиотеке. И они являются крайне уязвимой для атак социальной группой. На мой взгляд, необходимо включить блок основ информационной безопасности в состав дисциплины «Информатика» или же «Основы Безопасности Жизнедеятельности», где на простых и понятных примерах доступным языком будут объяснены простейшие правила сохранения конфиденциальности персональных данных и возможные последствия их раскрытия. Основы, которые будут даны в этих блоках, уже помогут уберечь детей от необдуманных и, попросту, опасных поступков. Закономерным будет включить дисциплину «Личная и корпоративная информационная безопасность» в программы обучения ВУЗов не только на связанных с ИБ специальностях, но и на всех прочих тоже. Это, в свою очередь, поможет сократить количество информационных инцидентов на предприятиях, в которые придут работать будущие выпускники.

К сожалению, столь значительные изменения в программах образования невозможно реализовать в сжатые сроки, которые диктует текущая ситуация. Одним из решений этой проблемы может являться организация факультативных занятий с привлечением студентов. Примером такой деятельности может служить лабораторный комплекс Центра освоения технологий информационного противоборства и борьбы за информационную живучесть объектов морской техники и морской инфраструктуры (ЦОТИП БИЖ ОМТИ), созданный по инициативе группы студентов СПбГМТУ при

поддержке Кафедры судовой автоматики и измерений, в котором регулярно проходят занятия по освоению современных технологий ИБ, а любой заинтересованный студент ВУЗа может получить консультацию по интересующей его теме. Не вызывает сомнений то, что и в других учебных заведениях, в которых имеются направления обучения, напрямую связанные с ИБ, найдутся неравнодушные студенты, которые даже при минимальной поддержке своей выпускающей кафедры смогут организовать подобные факультативы.

Но еще более значимым, по нашему мнению, является создание качественно новой информационной платформы моделирования – Полигона сетевого межвузовского взаимодействия (ПСМВ) для коллективной генерации и отработки совершенных алгоритмов защиты ресурсов, что позволит, безусловно, выйти и на качественно новый уровень защиты личной информации кроме традиционных и регламентированных персональных данных в контексте Федерального закона 152.

Калюта Н.Г.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

МЕТОДИКА ОЦЕНКИ ЖИВУЧЕСТИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЯ ПРИ БОЕВЫХ И АВАРИЙНЫХ ПОВРЕЖДЕНИЯХ

Современный уровень средств ведения вооруженной борьбы, постоянное присутствие ВМС вероятного противника в районах боевого предназначения, их высокая готовность к нанесению ударов по территории России обязывают Военно-морской флот быть в высокой степени готовности к отражению агрессии и выполнению стоящих перед ним задач. Одной из основных составляющих боевой готовности сил флота является готовность средств вооружения и технических средств.

К строящимся новым кораблям в настоящее время предъявляются к повышенные требования. Они вытекают из характера современного боя: его небывалых масштабов, быстротечности, насыщенности событиями, а главное - неизмеримо большей разрушительной силы нового оружия.

В этих условиях, с одной стороны, повышается ответственность за принимаемые командирами решения, а с другой - появляется необходимость вырабатывать эти сложнейшие решения в кратчайшие сроки.

В настоящее время объем информации, поступающей в распоряжение командира, управляющего боем, настолько велик, а изменения этой информации столь быстры, что он не успевает ее обрабатывать в нужном темпе и принимать своевременное решение. Это приводит либо к запаздыванию решения, либо к его недостаточной продуманности и обоснованности. Поэтому возникает весьма трудная задача, в короткий срок, измеряемый минутами, а порой и секундами, ознакомиться с обстановкой, проанализировать ее, принять решение и довести его до исполнителей.

Информационная поддержка при выработке решения означает переложение функций выработки решения на информационные системы. За командиром при этом остается безусловное право окончательного выбора (применения) решения, подготовленного информационной системой.

Для создания системы информационной поддержки необходимо разработать алгоритм работы такой системы.

Предлагается алгоритм оценки живучести технических средств корабля при боевых и эксплуатационных повреждениях.

В основу создания алгоритма предложена функционально-самостоятельная операция – операция, выполняемая основной корабельной системой с помощью одной или нескольких вспомогательных систем для выполнения поставленной задачи при получении кораблем боевых или эксплуатационных повреждений.

При наличии исходных данных, включая ограничение рассмотрения только сформированными задачами и выбранными техническими средствам (системами), технология автоматизированной оценки живучести включает в себя следующие основные этапы:

- разработка схемы деления корабля на аварийные (повреждаемые) участки и соответствующего ей перечня аварийных участков (АУ);
- создание таблицы возможных повреждений на АУ как базовых вариантов развития аварий;
- формулирование выполняемой для решения задачи группой технических средств (системам функционально-самостоятельной операции (ФСО) с выделением ее частных ФСО для технических средств (системам) из этой группы;
- описание функционально значимых элементов (ФЗЭ) выполнения сформулированной (и ее частных) ФСО, включая состав и характеристики стойкости основной аппаратуры, определяющей ФЗЭ;
- разработка функционально-топологической схемы расположения ФЗЭ;
- создание таблицы размещения ФЗЭ на АУ (ПУ);
- формирование множеств ФЗЭ, поврежденных поражающим воздействием при базовых вариантах развития аварии;
- разработка структурно-логической схемы выполнения сформулированной ФСО;

– определение непосредственных функциональных зависимостей между ФЗЭ сформулированной (и ее частных) ФСО;

– определение функциональных зависимостей между выходными ФЗЭ и сформулированной ФСО или ее частными ФСО;

– построение графа функциональных оценочных зависимостей (ГФОЗ) для сформулированной ФСО;

– вычисление на ГФОЗ расчетных значений показателей выполнения сформулированной (и ее частных) ФСО и показателей состояния ФЗЭ для базовых вариантов развития аварий;

– выделение и обоснование экспертом вариантов, при которых показатель выполнения сформулированной ФСО имеет нулевое расчетное значение, но имеются такие единичные расчетные показатели состояния ФЗЭ, при которых эта ФСО может быть считаться частично выполненной;

– принятие решения экспертом о достаточности выполненных вычислений для формулирования выводов о выполнении выбранными техническими средствами (системами) рассматриваемой задачи минимального уровня функционирования корабля;

– формулирование выводов по оценке живучести технических средств корабля при решении рассматриваемой задачи и необходимых рекомендаций по ее повышению.

Полученная таким образом информация получит оперативно получить информацию о возможности и режимах использования техническими средствам (системами) корабля.

Карпов А.Е., Алексеев А.В., Худобородов Е.Ф.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

АКТУАЛЬНОСТЬ КВАЛИМЕТРИЧЕСКОЙ ОЦЕНКИ ПРЕВОСХОДСТВА ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА СЛОЖНЫХ ЭРГАТИЧЕСКИХ СИСТЕМ

Анализ литературных и интернет источников последних лет в области информационных технологий управления объектами морской техники и морской инфраструктуры подтверждает, что назрела необходимость перехода от многочисленных публикаций к выполнению широкомасштабных научных исследований национальной проблемы обеспечения гарантированного превосходства информационно-управляющего пространства РФ (ЕИУП) по отношению ко всем потенциальным и реальным субъектам и объектам информационного вторжения. Одним из главных сегментов ЕИУП, безусловно, является ЕИУП Военно-морского флота в составе ЕИУП Вооруженных сил РФ.

В этом контексте одним из актуальных научно-методических вопросов после концептуальных аспектов развития ЕИУП, активно развиваемых в ВС РФ (Преснухин В.В., Протасов А.А., Соколов И.А., Чирков В.В., Николашин Ю.Л., Мирошников В.И. и др.), по нашему мнению, следует считать вопрос обоснования модели качества, измерения (квалиметрической оценки) и управления превосходством ЕИУП современных сложных организационно-технических человеко-машинных (эргатических) комплексов и систем (ЭТС), включая боевые информационно-управляющие системы ВМФ.

Создание модели и комплекса методик обеспечения превосходства в управлении ЭТС и в целом ЕИУП позволит практически разработчикам и эксплуатационщикам современных ЭТС результативно и эффективно решать сложнейшие задачи ситуационного и оперативного управления при использовании современных иерархических и сетецентрических ЭТС.

Более того, при обеспечении требуемых уровней верификации и валидности используемых данных квалиметрического оценивания превосходства ЕИУП реализация данной модели и комплекса методик позволит практически на основе многовариантного численного моделирования решать как задачи многокритериального и полимодельного анализа и вариантного синтеза, так и задачи оптимизации ЭТС по критерию максимизации превосходства в их управлении (МПУ).

Отсутствие на сегодняшний день комплексной целевой междисциплинарной программы исследования методов и средств построения систем управления, включая сетецентрические в ЕИУП распределенных и мобильных пунктов управления влечет за собой необходимость открытия комплекса НИОКР по созданию макетных образцов специализированных средств обеспечения МПУ и полигонов межсетевого взаимодействия по реализации так называемого сильносвязного ЕИУП в единые информационно-ударные комплексы и системы (ЕИУС).

В основу модели обеспечения превосходства ЕИУП критических объектов управления, к числу которых в полной мере относятся ЭТС ВМФ, предложено положить гармонический алгоритм агрегирования частных, групповых и модельных показателей их качества, как имеющий минимальную методическую погрешность оценивания в сравнении известными и широко используемыми аддитивным и мультипликативным алгоритмами.

Среди групповых факторов обеспечения превосходства ЕИУП предложено использовать:

– превосходство по комплексу функциональных возможностей, включая оперативность управления, достоверность используемых данных, устойчивость функционирования от внутренних и внешних источников естественного и искусственного происхождения (включая киберпротивоборство), скрытность (включая информационную, электромагнитную) и непрерывность функционирования;

– превосходство по комплексу эксплуатационных возможностей, включая качество освоения, обслуживания, резервирования, восстановления, экологичности и утилизации;

– превосходство по ресурсной обеспеченности (затратности), включая временную, финансовую, материальную, техническую, трудовую, социальную;

– превосходство по перспективности технологического развития, включая импотрозамещаемость;

– превосходство по времени принятия управленческих решений, их качеству;

– превосходство по лишению противника способности принимать решения и противодействовать;

– превосходство по адекватности восприятия противником оперативной, тактической обстановки;

– превосходство по рефлексивному управлению противником;

– превосходство в комфортности управления.

На примере по исходным данным Абрамовича А.В., Гужвы Д.Ю., Лихачева А.М. (2013 г.) по оценке состояния радиоэлектронной отрасли России показана критичность положения с интегральной оценкой потери превосходства в ЕИУП (1/4)0,2x(1/4)0,3x(1/3)0,2x(1/2)0,3=0,33 только с учетом соответственно состояний средств визуализации информации, проектирования и создания программного обеспечения, бортовых вычислительных комплексов и систем поддержки принятия решений.

Полученные оценки уверенно подтвердили актуальность форсированного решения проблемы обеспечения превосходства ЕИУП радиоэлектронной отрасли, а также научно-методического совершенствования аппарата квалиметрической оценки превосходства информационно-управляющего пространства сложных эргатических систем и, в первую очередь, ВМФ и других видов ВС РФ.

Карпов А.Е., Алексеев А.В., Худобородов Е.Ф.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ПРИНЦИПЫ И БАЗОВЫЕ КРИТЕРИИ ОЦЕНКИ ПРЕВОСХОДСТВА ИНФРОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА СЛОЖНЫХ ЭРГАТИЧЕСКИХ КОМПЛЕКСОВ

Традиционно сложной задачей исследования критических информационных технологий управления (ИТУ) объектами морской техники и морской инфраструктуры (ОМТИ) является формирование принципов их сравнения и критериев оценки. Тем не менее, с каждым годом и ростом насыщенности ОМТИ, их технологической сложности значимость этих вопросов только возрастает, а, тем более, в условиях, когда появился даже своеобразный термин – «проклятие сложности».

Вместе с тем, без качественного решения этой сложной многовариантной научно-методологической задачи практически невозможно обосновывать перспективные технологические решения и предложения по развитию ИТУ ОМТИ, а, тем более, по их оптимизации.

Со всей остротой эта проблема регулярно проявляется для ключевых национальных объектов, включая системы военного управления, в том числе автоматизированного управления ВМФ России.

Сегодня, в условиях решения национальной проблемы создания единого информационно-управляющего пространства (ЕИУП) ВС РФ, включая сегмент ВМФ, и обеспечения его гарантированного превосходства по отношению ко всем потенциальным и реальным субъектам и объектам информационного противоборства в киберпространстве как никогда востребованным является создание практических, доступных для широкого, можно сказать, повседневного использования модели и методик оценки превосходства в управлении различными ОМТИ, в том числе боевыми автоматизированными разведывательно-ударными комплексами и системами.

В известной литературе и интернет-ресурсах вопрос моделирования качества, а, тем более, оценки конкурентной способности ОМТИ и обеспечения превосходства ЕИУП постоянно поднимается, но реальных практических методов и методик, как нам известно, не предлагается.

В этой связи представляется целесообразным в развитие концептуальных подходов, в том числе развиваемых в публикациях Преснухина В.В., Протасова А.А., Соколова И.А., Чиркова В.В., Николашина Ю.Л., Мирошникова В.И. (авторов надо расширить и «обновить»), вопрос обоснования модели качества, измерения (квалиметрической оценки) и управления превосходством ЕИУП современных сложных организационно-технических человеко-машинных (эргатических) комплексов и систем (ЭТС), включая боевые информационно-управляющие системы ВМФ, рассматривать в следующем контексте и последовательности решения задач (выполнения исследований):

– разработки вербальной модели связи ключевых свойств превосходства в управлении (ПвУ) ОМТИ (оперативность, достоверность, устойчивость, скрытность, непрерывность) в условиях киберпротивоборства с ключевыми информационными свойствами ОМТИ (объем и скорость добывания и обработки информации, доля ценной для эффективного управления информации и т.п.);

– разработки модели шкалы оценки критерия превосходства (типа: соответствует базовому (требуемому) уровню (УТ), отставание/превосходство от УТ с относительным значением порядка

0,8/1,2 по критерию агрегированного (обобщенного, сводного) показателя качества (ОТ/ПТ), значительное отставание/превосходство от УТ с относительным значением порядка 0,5/2 (ОЗ/ПЗ), критическое отставание/превосходство с относительным значением порядка 0,25/4 от УТ (ОК/ПК);

– разработки математической модели оценки превосходства ЕИУП на основе обоснования алгоритма агрегирования частных (КПЧ) и групповых показателей конкурентного преимущества (КПГ) в агрегированный показатель превосходства (АПП) ЭТС ОМТИ, характеризующий их ключевое свойство - превосходство в управлении (ПвУ) ОМТИ;

– выполнения комплекса исследовательского проектирования на основе численного моделирования по обоснованию приоритетного ряда и оптимального варианта архитектурно-функционального построения и эффективного применения ЕИУП ВМФ с соответствующим технологическим обеспечением реализации данного комплекса обоснованных вариантов.

Исходным этапом решения поставленных задач является формирование системы базовых критериев оценки КПЧ и КПГ и АПП ЭТС и в целом АПП ЕИУП, в качестве которой предложены:

подсистема КПГ функциональных и эксплуатационных возможностей, а также ресурсной обеспеченности и перспективности технологического развития ЭТС ОМТИ на основе агрегирования соответствующих КПЧ с соответствующими индексами их критериальной значимости (весовыми коэффициентами) и альтернативно выбираемыми алгоритмами свертки КПЧ в КПГ;

подсистема КПГ принятия управленческих решений (по времени, их качеству с учетом степени прогнозной обеспеченности, с учетом эффективности автоматизированной информационно-аналитической и интеллектуальной поддержки в условиях активного киберпротиводействия и рефлексивного управления ЕИУП субъектов и объектов информационного вторжения).

Приведенные количественные оценки ПвУ ОМТИ показали целесообразность дальнейшего развития представленных положений замысла и научно-технических путей обоснования модели и технологии обеспечения гарантированного превосходства и создания ЕИУП ЭТС ОМТИ.

Коваленко Д.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА КОМАНДИРА АВАРИЙНОЙ ПАРТИИ ПРИ ПОДГОТЛОВКЕ К БОРЬБЕ ЗА ЖИВУЧЕСТЬ И ЕЁ ВЕДЕНИИ

Фактор времени при принятии решений в современных условиях является одним из основных показателей, определяющих возможность достижения цели.

Борьба за живучесть корабля представляет собой совокупность действий личного состава, направленных на поддержание и восстановление боеспособности поврежденного корабля.

Наиболее эффективными являются действия личного состава, проводимые на начальном этапе происшествия с кораблем. Командные пункты и боевые посты ведут борьбу за живучесть с помощью личного состава, приписанного к ним, согласно книги корабельных расписаний. Применение аварийных партий на этих командных пунктах, боевых постах, осуществляется при необходимости усиления личного состава КП (БП) или при его естественной убыли.

Основное предназначение аварийных партий - это борьба за живучесть в отсеках, помещениях корабля в которых отсутствует личный состав.

Подготовка и использование аварийных партий осуществляется согласно руководящих документов, утвержденных Главнокомандующим Военно-Морским Флотом. При подготовке и ведении борьбы за живучесть аварийной партией используются документация, разработанная согласно директивы ГК ВМФ ДФ-14 от 06.10.1992 года «О совершенствовании документации по руководству обеспечением живучести кораблей Военно-Морского Флота», в частности планшеты командиров аварийных партий надводных кораблей. В девяностые годы при отсутствии современных технологий планшеты соответствовали «духу времени» и позволяли улучшить подготовку аварийных партий. При этом в них были существенные недостатки: разработка планшетов личным составом корабля не имеющего проектно-конструкторской документации влекла за собой внесение иногда значительных неточностей в планшеты; размеры планшетов не позволяли оперативно использовать имеемый материал.

В настоящее время для ряда современных кораблей конструкторскими бюро разработаны планшеты на бумажных ламинированных носителях, выполненных в виде схем аварийных участков с описанием действий в виде пиктограмм (оценка обстановки, локализация и ликвидация аварии). Такие планшеты удобны с точки зрения информационной поддержки при подготовке аварийных партий к борьбе за живучесть корабля, так как несут информацию о аварийном участке, смежных с ним помещениях, системах, проходящих через аварийный участок, средствах борьбы за живучесть расположенных в аварийном и смежных отсеках, а также действиях личного состава по локализации и ликвидации аварии. Для применения их в ходе борьбы за живучесть не удобны, так как обладают значительными масса - габаритными показателями, пропорционально рангу корабля.

Для ведения борьбы за живучесть корабля наиболее рациональной системой информационной поддержки для командира аварийной партии является электронный планшет выполненный в

ударопрочном исполнении, загруженный контентом для подготовки личного состава аварийной партии и контентом для ведения борьбы за живучесть. Положительными свойствами электронного планшета являются: возможность использования в темном помещении; оперативность перехода (при необходимости) с аварийного участка на смежные помещения; возможность получения дополнительной, часто крайне необходимой информации по кораблю, личному составу и т.д.

Леберянский А.П.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ОБЩИЕ КРИТЕРИИ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ КОРАБЛЯ

На сегодняшний день являясь уникальным по сложности инженерным сооружением, боевой корабль остается одним из наиболее опасных в взрывопожароопасном отношении объектом.

Размещение в одном корпусе, казалось бы, несовместимых качеств:

огромной мощности главной энергетической установки, расположенной в замкнутом, малом объеме;

энергии воздуха высокого давления;

химических источников энергии;

средств регенерации;

различного вида оружия: ракетного, торпедного, артиллерийского, под которыми находится топливо.

И все это окружено электрической энергией большой мощности, токи которой достигают сотни килоампер, требуют совершенных конструктивных и организационно-технических решений, а при аварии правильных действий по БЖ всего личного состава.

Успех борьбы с пожарами на кораблях во многом зависит от умения офицерского состава разобраться в обстановке, оценить ее и немедленно принять меры, позволяющие локализовать и ликвидировать пожар. Для правильной оценки обстановки, принятия и реализации решений необходимо знать причины возникновения пожара, особенности его развития, в зависимости от конструктивных особенностей помещения, отсека и корабля в целом, имеемые возможности для его ликвидации с минимальным ущербом для корабля.

Применительно к кораблю, определение живучести корабля понимается, как способность корабля противостоять боевым и аварийным повреждениям, восстанавливая и поддерживая при этом свою боеспособность.

В отечественном кораблестроении вопросами обеспечения живучести уделялось постоянное внимание. Основоположником теории живучести корабля является вице-адмирал С.О. Макаров, который еще в 1875 г. определил живучесть как способность корабля продолжать бой, имея повреждения в различных боевых частях.

Искусство руководителя борьбы за живучесть состоит в том, чтобы с учетом качественной предварительной подготовки быть способным правильно оценивать аварийную ситуацию поврежденного корабля, ее последствия, возможный ход развития. Самому сознательно рассматривать и утверждать предлагаемые варианты действий или самостоятельно выбирать главное направление по БЖ и настойчиво добиваться реализации своих решений, сохраняя способность корабля решать поставленные задачи.

Общими критериями обеспечения живучести при оценке состояния поврежденного корабля являются:

- поврежденный корабль (отдельные ТТЭ утрачены) способен решать поставленную задачу;
- повреждения таковы, что поставленная задача не решается, но корабль может вернуться своим ходом;
- повреждения таковы, что возвращение своим ходом не представляется возможным и корабль нуждается в оказании ему помощи.

Основу частных критериев составляют оценки достаточности имеемых временных, прочностных, людских, материально-технических и др. ресурсов тем потребностям, которые могут иметь место в реальных условиях развития аварийной ситуации.

Максимова М.А., Петраков С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, ООО «Фарадей инжиниринг»
СОВРЕМЕННЫЙ ПОДХОД К ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ КОТЕЛЬНЫХ УСТАНОВОК

Котельная установка это комплекс технологических связанных тепловых энергоустановок, расположенных в обособленных производственных зданиях, встроенных, пристроенных или надстроенных помещениях с котлами, водонагревателями (в т.ч. установками нетрадиционного способа получения тепловой энергии) и котельно-вспомогательным оборудованием, предназначенным для выработки теплоты. Используются при централизованном тепло- и пароснабжении или при местном снабжении, если эта котельная локального значения.

При эксплуатации котельных установок средней мощности (например Viessmann, Buberus производства Германии и российских фирм, таких как Турботерм, Зиосаб) следует учитывать, что выполнение любого вида работ связанных с горелками должно выполняться специалистами сервисного центра, например сервис службами производителей Oilon, Weishauot, Riello. Следует обратить внимание на то, что в горелке и приборах автоматики нельзя менять установленные регулировки. Подобные изменения могут привести к серьезным последствиям. Также следует учитывать, что приобретение запасных частей дорогостоящее мероприятие и их доставка занимает значительное время.

Следует отметить, что на многих котельных установках техническое обслуживание ведется по календарному сроку, без учета фактического технического состояния отдельных узлов, что приводит к неоправданным технико-экономическим затратам.

В настоящее время, при возникновении аварийной ситуации происходит автоматическое выключение котла, с сигнализацией на пульт оператору. За это время может произойти значительное количество различных поломок, например: выход из строя топливных насосов, из-за забившегося фильтра или некачественного топлива; возникли повреждения топливной трассы и т.п.

В процессе эксплуатации если постоянно отслеживать определенные параметры, то повышается эффективность проведения ремонтов. В этой связи разработка системы технического обслуживания по фактическому состоянию и его алгоритма является актуальной и необходимой.

Как и любое сложное техническое оборудование, котел и горелка нуждаются в регулярном техническом обслуживании, призванном выявить: соответствие режимов работы и грелки заводским нормативам; наличие неполадок и нарушения в работе котла и горелки; устранить неполадки, произвести настройку и регулировку котла и горелки.

К комплектующим средствам аппаратной части системы технического обслуживания относятся: контроллеры, устройства для сопряжения контроллеров с датчиками и исполнительными механизмами, модули цифрового интерфейса , операторские станции и серверы системы, сети и автоматизированная система дистанционного управления (АСДУ) для передачи в диспетчерскую технологических параметров.

Поскольку техническое обслуживание котельной установки осуществляется специалистами удаленного сервисного центра, то они должны быть заблаговременно оповещены о предстоящей работе. Для этой цели можно использовать глобальную информационную сеть Интернет, по которой на компьютер автоматизированного рабочего места (АРМ) сервисного центра с компьютера АРМ котельной будут при необходимости в автоматическом режиме передаваться сообщения о прогнозируемой дате выполнения технического обслуживания и последние коды контроллера параметров технологического процесса. Данные коды позволяют выявить возможные причины нарушения технологического процесса.

В качестве контролируемых параметров, позволяющих осуществить прогнозирование времени выполнения технического обслуживания, можно использовать данные датчика давления топлива (P) на входе в котел и данные датчика температуры (T) отходящих газов. Поскольку эти параметры позволяют качественно оценить техническое состояние котельной, т.к. знание средней нормальной температуры отходящих газов и среднего расхода топлива позволяет оперативно выявлять отклонения от норм в работе котла и грелки.

Реальные функции P(t) и T(t) можно представить в виде временных рядов. Далее используя алгоритм управления работоспособностью элемента СЭУ [1], вычисляем сглаженные значения параметров и аппроксимирующие функции. Использую полученные аппроксимирующие функции выполняем прогноз наступления события при котором P(t) и T(t) достигнут допустимых значений.

Качество проведения технического обслуживания связано в первую очередь с диагностикой предаварийного состояния, во-вторых возможности существующих систем предсказывать ход развития аварийной ситуации. Из достоинств предлагаемой системы технического обслуживания можно выделить непрерывную диагностику состояния котельной до прогнозируемого момента наступления предаварийной ситуации.

Мозокин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СЕРВИСЫ, ТЕХНОЛОГИИ, УЯЗВИМОСТИ, УГРОЗЫ И ЗАЩИТА BLUETOOTH

Сегодня информационные технологии управления стремительно внедряются во все практически сферы нашей повседневной деятельности. Мы себе уже и не можем представить свою жизнь без смартфонов, компьютерной и бытовой техники. Но огромное количество проводов все еще мешает пользоваться устройствами с комфортом. В середине 90-ых компанией Ericsson была разработана технология Bluetooth. В конце 20-ого века компании Nokia, Intel, IBM, Toshiba и сам Ericsson образовали сообщество SIG (Special Interest Group), который разработал стандарт Bluetooth, без которого сегодня не может быть представлена наше информационное окружение.

Изначально технология была предназначена для того, чтобы избавится от лишних проводов. Допустим, если подсоединить к ноутбуку мышь, принтер и мобильный телефон с помощью проводов, то переносить его будет не очень удобно. Именно данная технология решает эту проблему. Все больше компаний выпускают Bluetooth продукцию. Технология Bluetooth применяется не только в компьютерной технике, но и в бытовой. Чайники, утюги, весы и кофеварки - всем этим можно управлять на расстоянии.

Вместе с тем, на новый план выходит актуальный вопрос систематизации видов атак, уязвимых для технологии Bluetooth,а так же вопрос эффективных технологии и средств защиты.

Когда используется Bluetooth для создания временной сети, компьютеры в этой сети взаимодействуют непосредственно друг с другом без участия беспроводной точки. Это значит, что нет централизованного места, где можно осуществлять контроль безопасности. Таким образом, обеспечение безопасности ложится на сами устройства.

Самая простая функция защиты Bluetooth - это перевод его в режим “Невидимый”. Когда устройство Bluetooth работает в режиме «Видимый», то можно легко произвести сканирование радиуса и найти это устройство при помощи PC (personal computer) и загрузить личные данные.

Перевод устройства в режим «Невидимый» предотвращает появление в списке сканирования. При соединении двух устройств, следует всякий раз защищать канал связи между ними с помощью средств аутентификации и кодирования.

Самое простое и главное правило безопасного применения этой технологии — выключать все, чем не планируется пользоваться. Если ноутбук, смартфон или планшет оснащены технологией Bluetooth и эти средства не используются, лучше отключить их. В таком случае никто не сможет использовать слабые места в настройках вашего устройства, а кроме того, это даст экономию энергии батареи. Тем, кто обращается к средствам Bluetooth лишь от случая к случаю, рекомендуется всегда отключать Bluetooth в ситуациях, когда они не используются.

Таким образом, можно отметить тот факт, что технология Bluetooth постоянно совершенствуется. Покрытие и скорость передачи данных увеличиваются с каждым обновлением. Так же каждый раз совершенствуются и расширяются возможности Bluetooth, например, система местоположения, а, следовательно, и не исключаются и возможности появления новых уязвимостей и угроз информационной безопасности.

Крупные и не только компании всё чаще прибегают к её использованию в своих сетях, новых технологических решениях, комплексах и системах. Это обязывает разработчиков и пользователей иметь ясные ответы на вопрос достигаемого уровня информационной безопасности и уровня защищенности ресурсов. Более того, это должно свидетельствовать о новом этапе исследований в части возможностей технологии Bluetooth и её защиты.

Мокин С.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ОРГАНИЗАЦИЯ ПОДГОТОВКИ АВАРИЙНЫХ ПАРТИЙ ГЭУ ПЛА

Для борьбы за живучесть технических средств ЯЭУ, локализации аварийных ситуаций с ЯЭУ, ликвидации их последствий при ухудшении радиационной обстановки в энергетических отсеках на пла должны быть сформированы и обучены аварийные партии реакторного отсека (далее – АП РО).

Состав аварийных партий реакторного отсека:

1. Командир АП (командиры групп дивизиона движения);
2. Старшина АП (машинист - трюмный РО);
3. Электрик АП;
4. Турбинист АП;
5. Нештатный дозиметрист.

По решению командира корабля в аварийные партии могут включаться и другие специалисты. Личный состав аварийных партий проходит специальную подготовку по БЗЖ технических средств ГЭУ в условиях ухудшения радиационной обстановки. Руководит подготовкой личного состава аварийных партий командир дивизиона движения с привлечением других командиров подразделений. За организацию подготовки личного состава АП РО отвечает СПК.

Подготовка аварийных партий РО должна быть направлена на изучение расположения систем и механизмов реакторного отсека и практическую отработку по выполнению необходимых переключений технических средств при локализации и ликвидации последствий аварийных ситуаций с ЯЭУ.

Организация подготовки АП РО определяет необходимый объём знаний и практических навыков л/с аварийных партий РО по организации, средствам и приёмам БЗЖ технических средств ЯЭУ при ухудшении радиационной обстановки. Подготовка аварийных партий РО проводится с использованием необходимых технических описаний и инструкций по эксплуатации систем и механизмов ЯЭУ, РБЖ-ПЛ-82, РБИТС-ПЛА, ПЭЭК-91, НОРБ ВМФ - 2004, РЭКУС-ПЛ, РБЯ ВМФ-2001, ПБЯ-В.08-88/05, ПБЖ ПЛ - 83 и др. Аварийные партии РО отрабатывается, как теоретически в

учебных кабинетах, так и при практических тренировках, непосредственно в реакторном отсеке, по использованию и переключению технических средств ЯЭУ.

Особое внимание должно обращаться на выработку у личного состава аварийных партий РО твёрдых практических навыков по использованию и переключению технических средств ЯЭУ, устранению неисправностей.

Подготовка личного состава АП РО проводится согласно недельного распорядка дня соединения (планирование подготовки АП РО проводится на учебный год). Контроль качества подготовки АП РО осуществляется СПК и командиром ЭМБЧ.

В соответствии с требованиями КППЛ отработку аварийных партий проводить по двухгодичному курсу. Теоретические занятия с личным составом АП РО проводить при отработке элементов курсовой задачи Л-1 в учебном центре. Практические действия отрабатывать на тренировках в пункте базирования с использованием материальной части.

Экипажи, обучение которых в учебных центрах 1 раз в 2 года планом БП не предусмотрено, программу подготовки АП РО (занятия и тренировки) отрабатывать в пункте базирования в полном объеме.

Личный состав АП РО должен знать:

1. Организацию, средства и приёмы БЗЖ технических средств ЯЭУ при ухудшении радиационной обстановки в объёмах, предусмотренных «Программами подготовки должностных лиц по ядерной безопасности, организующих эксплуатацию и эксплуатирующих объекты ВМФ с ЯЭУ» (ПРП-ЯБ-2005), программами подготовки по специальности, курсом общей подготовки.

2. Устройство реакторного отсека, общекорабельных механизмов и систем, проходящих через реакторный отсек, устройство парогенерирующего агрегата и систем его обслуживающих.

Личный состав АП РО должен уметь:

1. Вести борьбу за живучесть при аварии в РО (длительном полном обесточивании ЯЭУ, прекращении подачи питательной воды в ПГПГ, разрыве главного паропровода, разрыве 1 контура на неотключаемом участке, большом пожаре, затоплении забортной водой, наддуве), выполнять первичные мероприятия по борьбе за живучесть в РО, использовать средства БЗЖ в РО, проводить разведку РО, оценивать возможность использования технических средств РО при аварийных ситуациях.

2. Вскрывать реакторный отсек, АВ при аварии в РО и АВ. Включаться в индивидуальные средства защиты. Переключаться из одних средств защиты органов дыхания в другие. Контролировать р/а загрязнённость одежды, обмундирования и кожных покровов при покидании АП РО аварийного отсека. Проходить ПСО.

3. Отключать повреждённые участки систем ППУ. Отключать ПГПГ двойной запорной арматурой по воде и пару.

4. Производить переключения в системе ГВД, подключение резервной (запасной) групп, подключение ВВД на ГВД. Готовить к работе систему подпитки 1 к. от источников базы, цистерн питьевой и пресной воды.

5. Готовить систему на проливку активной зоны реактора. Вводить в работу систему расхолаживания (ремонтного) 1 контура.

6. Готовить к работе систему вакуумирования реакторного отсека. Пускать в работу компрессоры.

7. Готовить к работе систему вентиляции реакторного отсека. Снимать давление с реакторного отсека и АВ.

8. Обесточивать (подавать питание) на механизмы ППУ. Управлять арматурой систем ППУ с местного поста и вручную. Приготовить и управлять КР (КГ) вручную с местного поста.

9. Готовить к работе систему осушения и дренажа реакторного отсека на осушение ДЦ, НП РО.

10. Производить полную герметизацию реакторного отсека.

Москаленко В. А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ИНФОМАЦИОННАЯ ПОДДЕРЖКА КОМАНДИРА ПОДВОДНОЙ ЛОДКИ ПРИ БОРЬБЕ С ПОЖАРАМИ НА ПЛ

В процессе эксплуатации подводных лодок, ее живучесть обеспечивается тремя составляющими: конструктивными мероприятиями, организационно-техническими мероприятиями, действиями личного состава по борьбе за живучесть.

Под руководством борьбой за живучесть следует понимать циклично повторяющийся процесс воздействия руководителя борьбы за живучесть (органа управления) на пл, отсек, комплексы оружия или технических средств и экипаж, в котором последовательно, в реальном масштабе времени, на основании сбора и обработки информации о состоянии управляемого объекта, характера развития аварийной ситуации и оценки обстановки разрабатываются варианты решений направленных на достижение поставленных целей борьбы за живучесть.

Определяются меры для их реализации, организована и осуществляется передача управляющих воздействий на управляемый объект и организован контроль за их выполнением.

Если в процессе реализации принятого решения появляется новая информация о состоянии управляемого объекта, изменении характера развития аварийной ситуации и условий обстановки, производится коррекция принятого решения, разработка и передача новых воздействий на управляемый объект, выбранных из множества возможных альтернативных вариантов и обеспечивающих достижение конечной цели борьбы за живучесть при минимальном поражении или гибели личного состава, снижения боеспособности корабля и оптимальных затратах ресурсов.

Организатором и руководителем борьбы за живучесть являются в первую очередь командир пл. От его способности правильно оценить сложившуюся на поврежденной пл обстановку, выбрать главное направление борьбы за живучесть, своевременно принять решение, организовать и проконтролировать действия всего личного состава – зависит успех борьбы за живучесть.

Для исключения факторов затрудняющих принятие решения на борьбу за живучесть (особенно борьбу с пожарами) необходимо информационное обеспечение решения следующих проблем:

- обеспечение достоверной информации о состоянии пл в первые моменты после пожара;
- исключить дефицит времени на добывание, обработку информации и принятие решения;
- прогнозирование возможного развития аварии.

Происшедшие с пл ВМФ катастрофы и тяжелые происшествия показывают, что большинство из них могли бы быть предотвращены или локализованы и ликвидированы без тяжелых последствий при информационной поддержкой должностных лиц находящихся на мостике, главном командном пункте корабля или командных пунктах боевых частей и служб.

Сформулируем основные проблемы информационной поддержки борьбы с пожарами сложных технических систем и управления ими при борьбе за живучесть, осуществляемой с целью сохранения возможных уровней работоспособности:

- неопределённость о времени, месте, размере, продолжительности, интенсивности и физической природе поражающего воздействия;
- возможны комбинации различных по своей природе поражающих воздействий, возникающие, как правило, последовательно во времени, когда первое поражающее воздействия, производя разрушения отдельных конструктивных узлов, агрегатов и механизмов, «вызывает» поражающие воздействия другой природы;
- заранее непредсказуемый при воздействии поражающего воздействия объём повреждений компонентов технических средств, непредсказуемость комбинаций первичных повреждений и сочетаний отказов компонентов различных комплексов ТС;
- возможность каскадного развития повреждений и отказов во взаимосвязанных многоагрегатных комплексах технических систем, возникновение вторичных повреждений;
- неопределённость ситуации и непредсказуемость конечных последствий каскадного развития аварий в комплексах технических систем;
- неполнота, недостоверность и быстрое устаревание информации об аварийной обстановке, о параметрах поражающих воздействий;
- сильное влияние на уровень живучести топологии автоматизированных комплексов технических систем;
- потребность принятия решений или автоматической выработке управляющих воздействий в «незапланированных» или нестандартных аварийных ситуациях;
- проблематичность выработки решений по переключениям технических систем.

Никитин А.Г.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ОСНОВНЫЕ НЕДОСТАТКИ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ СОВРЕМЕННЫХ КОРАБЛЕЙ ВМФ

В настоящее время в состав ВМФ вошел новый корабль ВМФ. В процессе строительства, сдачи, государственных испытаний корабля были выявлены существенные недостатки обеспечения живучести корабля, технических средств, обитаемости. Некоторые из них представлены ниже:

1. Помещение линий вала: Вход в помещения линии вала, ЭПЖН, ВОН № 3 один вертикальный трап длиной 7,2 метра, спуск личного состава затруднен, травмоопасен (особенно при качке, ведении БЗЖ). Необходимо разработать конструктивные изменения на установку аварийного или запасного входа выхода из помещения валолиний (бронедверь). Для обхода помещения не предусмотрены специальные трапы и лазы, что неизбежно приведет к травматизму личного состава, особенно при вращении валов. В устройстве валолинии отсутствует ленточный стопор, что не позволяет использовать ГЭУ в режиме с застопоренной валолинией. ВПУ используется для проворачивания валолинии, а не ГДГД. Связь с КП находиться на носовой переборке, а органы управления ВРШ через валолинию посередине помещения.

2. Машинное отделение: Расстояние между ГД № 1 и ГД № 2 составляет 1,02 метра, что не позволяет произвести качественное обслуживание дизеля, особенно при нахождении корабля в море.

Расположение пультов управления ГДГД, ВРШ, ГГС, АС-МТТ расположены не в одном месте. Нет закрытого аварийного выхода из машинного отделения с палубы платформы.

3. Отделение дизель - генераторов: Трубопровод системы пенотушения расположен на высоте 1,4 метра от настила палубы, что неизбежно приведет к травматизму личного состава. Местный пост БП отделения дизель - генераторов (средства связи) расположен в значительном удалении от местного поста управления ДГ № 3, 4. Местный пост управления ДГ № 3, 4 расположены слишком низко, в связи с чем управление дизелями становится неудобным, особенно в условиях качки. В помещении имеется всего один сход со второй палубы на платформу, расположенный с противоположного борта от входа в отделение. Нет закрытого аварийного выхода из отделения дизель - генераторов с палубы платформы.

4. Котельное отделение: Местный пост управления электрокомпрессора ЭКСА-7,5 в помещение электрокомпрессора расположен слишком высоко, проход вокруг ЭКСА-7,5 узкий. Патрубки осушительной системы находятся над колодцами, а не в них, что приводит к постоянному наличии воды в трюмах. Нет закрытого аварийного выхода из отделения дизель -генераторов с палубы платформы.

5. Обитаемость личного состава: В ВК №9 унитаз расположен таким образом, что закрыть дверь, зайдя в помещение невозможно. В каютах отсутствуют шкафчики для бритвенных и умывальных принадлежностей. Уровень шума вентиляции очень высок. Многие двери открываются в сторону коридора. Проход личного состава затруднен.

6.ГКП. Место нахождения рулевого расположено на значительном удалении от поста управления рулем. Нижний край иллюминаторов расположен высоко, достаточной обзор осуществляется только при нахождении в непосредственной близости наблюдающего к иллюминаторам, с рабочего кресла командира корабля и вахтенного офицера горизонт не виден.

7. А так же: Помещения МО, ДГО КО. На расстоянии 0,5-1,0 м от трюмов находятся стойки системы автоматического управления ГДГД, ДГДГ, ВКУ. Система управления ВРШ «Радуга». Истинный угол поворота лопастей ВРШ в положении «СТОП» соответствует значению «-27,4 град». Что бы дойти до ДГ №3,4, ЭКСА7,5-3М-1 нужно пройти по периметру все ДГО с левого борта на правый борт. Нет аварийного выхода из рулевой машины (в наличии один вход с юта по вертикальному трапу) и т.д.

Указанные недостатки в ходе строительства, недоработки, исполнение с низким качеством чертежей РКД, многочисленные ошибки, допущенные КБ-проектантом в ходе проектирования, привели к внесению в проект корабля значительного количества изменений, выполняемых в ходе постройки и сдачи корабля. А так же государственная комиссия составила протокол предложений по улучшению боевых и эксплуатационных качеств при строительстве следующего корабля.

Панфилов М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ МЕТОДОВ ПРИМЕНЕНИЯ SQL-ИНЪЕКЦИЙ И МЕР ПО ИХ ПРЕДОТВРАЩЕНИЮ.

SQL инъекция – это один из самых распространённых способов взлома сайтов и программ, работающих с базами данных, а также самих баз данных, основанный на внедрении (инъекции) в запрос произвольного SQL-кода. С помощью таких инъекций хакер (злоумышленник) может получить полный доступ к базе данных атакуемого и, таким образом вскрыть всё её содержимое, отредактировать или даже удалить.

По известной статистике от Hackmageddon, на все успешные атаки проходятся 19% SQL-атак. Это самый высокий показатель среди известных методик взлома.

Если упрощенно описывать SQL инъекции, то получится примерно следующее: Отец, написал в записке маме, чтобы она дала Васе 100 рублей и положил её на стол. Переработав это в шуточный SQL язык, мы получим:

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Васе

Её увидел брат Васи - Петя. Петя, будучи хакером, дописал там «ИЛИ Пете» и получился такой запрос:

ДОСТАНЬ ИЗ кошелька 100 РУБЛЕЙ И ДАЙ ИХ Васе ИЛИ Пете

Мама, прочитав записку, решила, что Васе она давала деньги вчера и дала 100 рублей Пете.

Вот такой простой пример SQL инъекции из жизни. Однако, если бы мама догадалась сравнить почерк или бы отец догадался поставить жирную точку в конце предложения, то такой “взлом” не увенчался бы успехом.

А вот уже и рабочий пример уязвимого кода (PHP):

```
  $user = $_GET['user'];
$query = "SELECT * FROM news WHERE user='$user'";
```

В данном коде специальные символы не фильтруются и злоумышленник может воспользоваться этим. Если рассмотреть подробнее, то видно, что в переменную user передаётся

значение, которое потом передаётся в запрос (query). Исходя из запроса, можно сделать вывод, что этот код получает все данные из таблицы news, в которых есть упоминание о введённом нами запросе. Но в переменной user также можно передавать всё, что угодно, например, " '; DROP TABLE news; --' ". Тогда наш запрос будет выглядеть так: "SELECT * FROM news WHERE user=' '; DROP TABLE news; --' '', что приведёт к полному удалению таблицы news. Тем самым, мы без лишних проблем удалили целую таблицу. Чтобы сделать наш код безопасным, можно воспользоваться стандартными методами защиты в языке PHP. Безопасный код будет выглядеть так:

```
$user = mysql_real_escape_string($_GET['user']);
$query = "SELECT * FROM news WHERE user='$user'";
```

Оператор mysql_real_escape_string сделает из специальных обычные символы, не влияющие на синтаксис запроса. Однако, и такой метод не безопасен, он недостаточно фильтрует данные, из-за чего, с трудом, но использовать SQL инъекцию можно.

Только в одной из самых популярных CMS (Content management system), WordPress, как известно, за последний год было найдено 10 уязвимостей, используя которые можно произвести SQL инъекцию. На базе данной CMS работают тысячи веб ресурсов, и далеко не все они обновляются своевременно. Трудно даже представить сколько тысяч (миллионов?) веб ресурсов может быть подвержено данной атаке.

Примерно так же обстоят дела и у ещё одной популярной CMS, Joomla, в которой только за этот год нашли уже 6 SQL-уязвимостей.

Наличие таких уязвимостей ставят под сомнение любой веб ресурс поскольку потенциальный хакер (злоумышленник) сможет получить доступ ко всем данным владельца, к личным данным его клиентов, сотрудников и воспользоваться ими по своему усмотрению. Например, продать их, или отредактировать со своей целью.

Основные методы борьбы с SQL-инъекциями заключаются в фильтрации специальных символов, которые используются в синтаксисе SQL-языка. Обычно, фильтрация происходит на стороне сервера: либо стандартными средствами самого языка программирования, либо с помощью специально написанных для этого библиотек. Реже программист сам пишет средства для фильтрации запросов.

Однако, непосвященному человеку в угрозах безопасности так же можно избежать взлома и утечки данных, для чего достаточно использовать уже готовые решения (Drupal, ocPortal, WordPress), и своевременно их обновлять В этом случае риск взлома будет минимальным.

В докладе раскрываются актуальные вопросы, связанные с SQL инъекциями, статистики взломов и найденных уязвимостях на популярных ресурсах и CMS, существующие на данный момент уязвимости, способы выявления уязвимостей и предотвращения их появления. Приведены примеры взлома, а также защиты и утилиты, позволяющие всё это автоматизировать. Показаны возможности, открывающиеся перед хакером, нашедшим SQL уязвимость, опасности, которые ждут разработчика при разработке ПО или Веб ресурсов.

Поленин В.И., Можаева И.А., Потехин А.А., Сущенков Д.А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»,
ООО НТЦ «Севзапмонтажавтоматика»

СОВЕРШЕНСТВОВАНИЕ ПРОГРАММНЫХ КОМПЛЕКСОВ АВТОМАТИЗИРОВАННОГО СТРУКТУРНОГО МОДЕЛИРОВАНИЯ С ПРИМЕНЕНИЕМ ОЛВМ ПО ВЕРОЯТНОСТНОЙ ОЦЕНКЕ ТЕКУЩЕЙ И ИТОГОВОЙ УСТОЙЧИВОСТИ БОЕВЫХ И ТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПОРАЖАЮЩИХ ФАКТОРОВ

Проблематичность вопроса применения теории вероятностей в моделях вооруженного противоборства и функционирования опасных производственных объектов (ОПО), отражающих развитие событий во времени, состоит в том, что итоговые события, исходы вооруженного противоборства и функционирования ОПО как результат применения немонотонных моделей, характеризуются реализацией случайных величин, в общем случае с немонотонной функцией текущего времени. Смысл этой функции характеризует текущую вероятность осуществления соответствующего немонотонного события.

Постановка задач на моделирование вооруженной борьбы и функционирования ОПО обычно связана с вычислением вероятностей исходов вооруженного противоборства и функционирования ОПО как в функции текущего времени, так и по завершении модельного времени. Немонотонность вероятностных функций исхода противоборства порождает логическую проблему оценки финальных значений показателей исхода.

В статье рассматривается путь решения этой проблемы на основе простейшей модели вооруженного противоборства (дуэли) с производством сторонами по одному выстрелу.

С применением методов теории вероятностей вычисляется вероятность события, состоящего в том, что на заданном интервале времени сторона 1 выстрел произвела, а сторона 2:

1. либо выстрел не произвела;

2. либо выстрел произвела позже стороны 2.

Именно это сложное событие характеризует поражение противника или риск потери устойчивости опасного производственного объекта.

В программном комплексе ПК АСМ 2001 эта модель и расчетная методика реализованы для экспоненциального закона распределения и единичного акта воздействия поражающего фактора.

Определены два направления дальнейшего совершенствования этого аппарата в составе ПК АСМ:

1) наряду с экспоненциальным законом разработать технологию модельной реализации нормального закона распределения времени нанесения ударов, возникновения опасных факторов, который в большей степени соответствует характеру временных процессов данного типа;

2) поскольку актов дуэлей, обмена ударами в модели вооруженного противоборства может быть несколько, необходимо серию функциональных вершин со специально выделенными постоянными номерами размножить некоторым образом, либо путем расширения количества постоянных номеров, либо путем индексации одной такой группы.

Разживин Н.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

УЧЕБНО – ТРЕНАЖЕРНЫЙ КОМПЛЕКС ЦЕНТРА ОСВОЕНИЯ ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Вопросы обеспечения информационной безопасности объектов информатизации, в том числе объектов морской техники и морской инфраструктуры (ОМТИ), приводят сегодня к необходимости расширения форм их организации. А именно - комплексной организации защиты информационных ресурсов и интересов пользователя в целях достижения информационного превосходства над информационным противником, как «инициаторов» информационных инцидентов, нарушителей режима обеспечения информационной безопасности (ОИБ).

При этом – комплексной организации защиты информационных ресурсов (ИР) не только в традиционном понимание пассивной защиты своих ИР («самообороны»), но и в контексте прямого активного противоборства с «инициаторами» («вторженцами») информационных атак (ИА) и активного информационного противоборства (ИП).

Практика показывает, что гарантированное информационное превосходство может быть обеспечено только при комплексном использование всех форм организации (пассивных и активных) и всех возможных методов организации и технологий защиты информации (ОТЗИ).

В этих условиях актуальной становится тема обоснования структуры, свойств и требований к специализированным средствам подготовки специалистов при организации мероприятий как ИБ, так и информационного противодействия (ИПД), а также в целом информационного противоборства (ИП).

В этой связи в Санкт-Петербургском государственном морском техническом университете был создан Центр освоения технологий информационного противоборства (ЦОТИП), в котором одна из задач - подготовка специалистов по направлению информационная безопасность. Для лучшего взаимодействия был разработан специализированный Учебно-тренажерный комплекс (УТК) с системой поддержки принятия решений. Основными задачами УТК ЦОТИП являются:

- сетевое обеспечение решения задач освоения технологий ИП, включая новые;
- учебно-тренажерная отработка практических навыков, как по ИБ, так по ИПД и ИП в целом;
- контроль выполнения заданий, как индивидуально каждого обучаемого, так и в составе специальных групп ИП, включая группу участников соревнований CTF;
- обеспечение моделирования сложных ситуаций информационного взаимодействия и подготовки обучаемых в этих ситуациях и другие.

Внедрение в образовательную систему новых компьютерных технологий позволяет продуктивно решать стоящие перед ней задачи. Совокупность средств и методов, которые используются для достижения поставленной цели, составляет информационно-методическое обеспечение (ИМО) процесса подготовки специалистов в области информационного противоборства.

Требования к качеству практической подготовки специалистов по обеспечению ИБ, ИПД и ИП растут и это предопределило актуальность создания УТК ЦОТИП, обеспечивающего подготовку студентов, магистрантов, аспирантов и преподавателей, а так же переподготовку специалистов в системе Дополнительного профессионального образования, обладающих необходимыми для этого компетенциями.

В докладе выполнен сравнительный анализ современных технологий ИП применительно к типовым условиям ОМТИ типа ЦОТИП, обоснованы предложения по новому варианту организации освоения технологий ИБ и ИПД применительно к типовым условиям ОМТИ.

Кроме того, выполнен анализ уязвимостей и угроз ИБ и ИПД ОМТИ типа ЦОТИП, как учебно-модельного аналога ОМТИ, показано, что риск угроз ИП может составить более 1,15 млн. руб.

Приведены и обсуждены разработанные 3 сценария управления ИП для УТК ЦОТИП, а также разработанная Методика и Руководство использования макетного действующего образца «СПРУ-УТК».

Представлены результаты выполненной адаптации известной технологии «СПРУ» к условиям УТК ЦОТИП, а также произведенной технологической отработки сценариев МДО «СПРУ-УТК».

В результате данного этапа работ выполнена комплексная оценка качества, конкурентной способности и перспективности развития технологий и макетного действующего образца УТК ЦОТИП.

В составе сформулированных предложений по дальнейшему развитию УТК ЦОТИП:

- расширение базы данных сценариев ИП и борьбы за информационную живучесть (БИЖ) ОМТИ с последующей актуализацией базы данных с их ранжированием по уровню угроз;
- создание реестра и демонстрационного стенда средств ИБ, ИПД и ИП в целом на базе технологий и УТК ЦОТИП для обеспечения комплекса специальных практических и лабораторных работ;
- включение УТК и ЦОТИП БИЖ ОМТИ в целом в предлагаемую для создания систему и Полигон сетевого межвузовского взаимодействия (ПСМВ) для системного моделирования в условиях, максимально приближенных к реальным, комплекса сценариев ИБ, ИПД и ИП в целом.

Рябцев М.Д.
Россия, Санкт-Петербург , ГУМРФ им. адм. С.О. Макарова

ИСТОРИЯ РАЗВИТИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПЕРЕВОЗКАМИ И РАБОТОЙ ФЛОТА В РОССИЙСКОЙ АРКТИКЕ

Все больше внимания ВМФ привлекает такой регион, как Арктика, где сосредоточены богатейшие биоресурсы, запасы углеводородов и других полезных ископаемых. В связи с этим возникает много вопросов в направлении движения развития Арктической зоны РФ и СМП в целом. В связи с этим требуется многолетний план по усовершенствованию ледокольного флота РФ.

Салащенко А.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В ЗАДАЧАХ ЛОКАЛИЗАЦИИ АВАРИЙНЫХ СИТУАЦИЙ

Развитие электронной вычислительной техники приводит к быстрому проникновению новых приемов и методов, связанных с этой техникой, в сферу многочисленных отраслей. Во многих случаях новые возможности позволяют осуществлять поиск результатов, ранее недоступных. Примером может быть развитие методов линейного программирования, сетевых методов, статистических исследований и многих других, практическое применение которых неразрывно связано с электронной вычислительной техникой.

В общих чертах исследование сложных объектов может быть реализовано:

- методами, вытекающими из современного состояния теории объекта;
- экспериментальными методами.

Оперируя теорией объекта, мы пользуемся его моделью, образовавшейся в результате формализации описания объекта способом, представляющим возможность применения определенных математических теорий.

Понятие модели связано со способом реализации экспериментальных исследований. Таким образом, моделью будем считать описание объекта, преобразованное в программу для ЭВМ, которая после выполнения дает результаты, позволяющие извлечь соответствующие предложения, касающиеся деятельности реального объекта. Экспериментирование с моделью назовем имитацией, так как во время прохождения экспериментов модель как бы изображает (имитирует) деятельность реального объекта. Модели, созданные для целей, связанных с имитационными исследованиями, назовем имитационными моделями.

Вышеупомянутые определения поясняют имитационное моделирование как метод исследования реальных объектов, основывающийся на экспериментировании с их моделями, представленными в виде программ для ЭВМ.

Следовательно, недостатки теории реальных объектов в известной степени устраняются теорией и практикой эксперимента на моделях объектов при использовании соответствующей техники вычислений (программ), а также электронных машин в качестве инструмента исследования.

Очевидно, что эксперименты не ведут непосредственно к созданию теории исследуемых объектов, однако на основе их результатов могут быть созданы гипотезы, впоследствии подтверждаемые теоретическими изысканиями.Упомянутые выше объекты рассматриваются как системы локализации аварии нарастающей сложности (ЛАНС).

Разумеется, эти же объекты могут анализироваться и в разных других плоскостях, но в данной работе мы ограничимся лишь теми аспектами их деятельности, которые можно рассматривать в категориях систем ЛАНС.

Вышеприведенное определяет объект, исследуемый методами имитационного моделирования, как сеть, фрагмент или элемент БЗЖ, который совместно с задачами и противоаварийными процедурами трактуются как системы ЛАНС.

Ограничившись рассмотрением управления развитием аварийной ситуации, можно выделить следующие области применения методов имитационного моделирования:

- в проектировании;
- в анализе существующих решений;
- в управлении.

Это деление во многих случаях нечеткое. Например, проектирование реконструкции, оснащения и организации деятельности реальных объектов (систем) может рассматриваться как анализ существующих решений в измененных условиях работы. В свою очередь анализ деятельности реальных объектов в условиях увеличения требований, поставленных перед ними, предшествует решению, ведущему к этим изменениям, и является элементом управления.

Можно утверждать, что методы имитационного моделирования, берущие за исходные данные реальные состояния систем, наиболее часто применяются на практике и ведут к эффективным решениям. Все они, в общем, сводятся к выбору наивыгоднейших:

- изменений оснащения и организации деятельности системы с учетом поставленных перед ней заданий;
- заданий для системы с учетом существующих оснащения и организации деятельности;
- комбинаций изменений оснащения, организации деятельности и заданий для исполнения.

Понятие наивыгоднейшего решения относится к группе изучаемых решений, из которых в соответствии с определенными критериями отбора выбрано одно решение. Таким образом, рассматриваемые методы всегда связаны с многовариантным поиском. Кроме сделанных выше оговорок, применение методов имитационного моделирования в проектировании, анализе существующих решений и управлении отличается спецификой, позволяющей выделить характерные свойства этих методов.

Методы имитации в проектировании являются часто единственно доступными для оценки будущего поведения системы без действительного внедрения проекта. Наиболее целесообразными являются анализ и оценка в фазе предпосылки или предварительного проектирования.

При исследовании системы обычно рассматривают следующие вопросы:

Гарантирует ли взаимозависимость всех элементов достижение целей (реализацию заданий), поставленных перед проектируемой системой?

С какими побочными явлениями, т.е. с какой устойчивостью на изменения предполагаемых продуктивности и организации, достижима реализация целей?

Где находятся критические точки, которые обусловливают продуктивность всей проектируемой системы?

Выявленные особенности проекта позволяют в общем осуществлять изменения в оснащении и организации, приводящие к достижению цели с меньшими затратами. А возникший таким образом вариант проекта требует новых имитационных исследований.

При стремлении к своеобразной оптимизации, основывающейся на целенаправленном повторении исследований некоторого числа вариантов и выборе наиболее рационального из них, цикл исследований может быть повторен многократно.

Выявленные особенности проекта позволяют осуществить изменения в предпосылках, которые ведут к лучшему подбору элементов для совокупности системы. Подбор происходит в ряде экспериментов (имитациях) с моделью при изменениях каждый раз предпосылок и сводится к целенаправленному анализу некоторого числа вариантов и выбору наиболее рационального с точки зрения цели, поставленной перед системой.

Как вытекает из вышесказанного, в одном проекте системы обычно появляется потребность обработки ряда моделей и выполнения, имитационных исследований при многократно изменяющихся условиях. Методы имитации в анализе существующих решений позволяют исследовать реальные системы с учетом связей между их элементами, а также между системой и внешней средой. Экспериментальные исследования в этом случае осуществляются, не нарушая деятельности системы, поскольку проводятся на отражающей ее модели.

Непосредственной целью исследования может быть:

- обнаружение явлений, происходящих в системе, а особенно выявление ограничений, противоречий, критических точек и сечений;
- исследование влияния единичных изменений в характеристиках элементов на деятельность всей системы;
- исследование влияния единичных изменений в связях (организации) на условия деятельности элементов и системы как их совокупности;
- исследование деятельности системы в измененных условиях взаимодействия с внешней средой, определяемой в качестве высшей системы.

Когда целью является выявление изменений, совершенствующих деятельность системы, различие между анализом проекта и исследованием реального объекта стирается. Цель в таком случае достигается рядом последовательных имитационных исследований. Данные получаются на основе измерений и анализа аварийности ПЛА. Некоторые из решений могут быть проверены тем же самым способом.

В результате модификация существующих решений, подкрепленная имитационными исследованиями, оказывается чрезвычайно эффективной и уменьшает риск совершения ошибки на корабельном или штабном уровнях.

В этих случаях методы имитационных исследований оказываются незаменимыми. Их использование раскрывает действительный объем сведений о системе, ведет к упорядоченным наблюдениям и измерениям.

В результате ГКП получает сведения о состоянии системе и рекомендации для локализации ситуации в кротчайшие сроки, недостижимые другими путями.

Наиболее существенным достижением имитационных исследований при анализе реальных решений является возможность быстрого получения обоснованных ответов на вопросы о том, как поведет себя система при изменении условий взаимодействия с внешней средой. Для этого достаточно изменить данные в программе имитации деятельности системы, что в свою очередь создает возможность подготовки универсальных программ для конкретных областей применения, объединенных в электронные базы данных.

В итоге последствия решений более широкого характера могут быть детально проанализированы перед их реализацией.

Методы имитации в управлении позволяют осуществлять исследование результатов планируемых решений перед их передачей исполняющим органам. Моделированием исследуют варианты планируемых решений, не нарушая деятельность реальной системы.

На основании проведенных исследований не только выбирается наиболее выгодное решение, но результаты имитации расширяют и углубляют сведения о предполагаемых последствиях реализации выбранных решений.

Управление по отношению к системе сводится к получению решении:

- изменяющих задачи системы;
- корректирующих ее деятельность.

В первом случае задачи системы подлежат изменению из-за введения новых условии взаимодействия системы с внешней средой. Применение методов имитации в управлении сводится к проверке деятельности системы в измененных условиях и оценке необходимых модификаций. Это не выходит за пределы анализа реальных решений.

Другой случай касается деятельности системы. Отклонения от принятой нормы деятельности ведут к неполной реализации заданий. Причины, вызывающие отклонения и имеющие по отношению к системе случайный характер даже т

огда, когда они проанализированы на фоне более широкого окружения системы (внешней среды), не являются случайными. Решения ведут к корректировке деятельности системы, чтобы дать возможность полной реализации заданий при наименьшей себестоимости.

Корректирующие действия могут быть предприняты через более короткое время по сравнению со временем, в течение которого происходят изменения в системе, существенные с точки зрения необходимого процесса. В таком случае принятие очередных решений, освобождающих от корректирующих действий, является текущим управлением (в реальном масштабе времени).

Корректирующие действия могут быть предприняты в то же самое время, в которое происходят изменения в системе. В таком случае принятие решений, освобождающих от корректирующих действий, является планированием. Планирование предполагает достижение системой предусматриваемого состояния в определенном периоде времени.

Разница между планированием и текущим управлением стирается в системах с большим опозданием и дискретностью передачи информации.

Применение методов имитации сводится к анализу многих вариантов планов и выбору наиболее эффективных с точки зрения корректирующих действий. Имитацией охватывается ближайший период деятельности системы, достаточный для оценки искомых решений.

Использование имитационных программ происходит упорядоченным способом. Упорядочивающим фактором является организация управления, в которой имитационные методы должны быть соответственно учтены. Это создает возможность подготовки программ имитации в виде своеобразных библиотек, эксплуатируемых непрерывно.

Введение имитационных методов моделирования требует изменений в организации управления, использования новых методов управления и планирования. Однако полученное в результате увеличение четкости управления в сложных и динамических системах с избытком возмещает донесенные затраты.

Свиньин С.Ф., Алексеев А.В., Попов А.И., Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный морской технический университет, Северный (Арктический) федеральный университет имени М.В. Ломоносова

ТЕОРИЯ ИНФОРМАЦИИ: ОТ ТЕОРЕМЫ УКШ К ТЕОРИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ

30 апреля 2016 года исполнилось 100 лет со дня рождения Клода Э́лвуда Ше́ннона.

В канун знаменательной даты в Санкт-Петербургском институте информатики и автоматизации Российской академии наук состоялось специальное заседание ученой общественности, посвященное этому событию. На юбилейном семинаре были заслушаны доклады о научной биографии основателя современной теории информации К. Шеннона, основных его заслугах в области теории связи и теории информации. Отмечено, что фундаментальная теорема отсчетов в теории информации не утратила своей актуальности и сегодня, имеет ряд вариантов современной трактовки.

Принцип финитности спектров по-прежнему является одним из определяющих граничные условия перехода к дискретным сигналам и их цифровой обработке, для исследования которых все большее применение находит целый спектр методов функционального анализа.

Энергетические пространства, сигналы с конечной энергией, функции с компактными носителями широко используются сегодня в арсенале исследовательских средств. Представление модели сигналов функциями времени конечной длительности, а также использование вейвлет-базисов и обобщенных алгоритмов быстрых спектральных преобразований позволяют сегодня решать самые сложные задачи тонкого спектрального, кепстрального анализа и других.

Участникам юбилейной встречи были представлены целый ряд современных методов исследования тонкой структуры сигналов, включая анализ биомедицинских сигналов большой длительности. Применение теории отсчетов при изучении двигательной деятельности органов желудочно-кишечного тракта человека, анализе результатов цифровой электрогастроэнтерографии с различными диапазонами и полосами гармонического анализа позволяет сегодня результативно решать конкретные практические задачи диагностики заболеваний и прогнозирования их динамики.

Особое внимание участников юбилейной встречи было уделено анализу фундаментального значения теоремы отсчетов Уиттекера-Котельникова-Шеннона (теоремы УКШ), развитие которой, по мнению участников, насчитывает сегодня более пяти исторических этапов, включая:

- «математический период» выявления закономерности представления временных функций массивом выборочных значений, кардинальной функцией интерполяции (E.T. Whittaker);
- «телеграфный период» освоения выявленной закономерности в прикладных областях знаний и практической деятельности (H.Nyquist, В.А. Котельников);
- «связной период» обобщения закономерности и теоремы отсчетов для задач связи при наличии шума и перехода к информационной парадигме (К. Шеннон);
- «интерферренционный период» обобщения закономерности и теоремы отсчетов с учетом и контролем мощности помех наложения спектров (мимикрии частот, алайзинга и т.п.);
- «оптимизационный период» спектральной интерпретации процессов дискретизации и квантования с обобщением теоремы отсчетов на основе учета специфики, динамического диапазона и погрешностей преобразования полосовых финитных процессов с возможностью оптимального («двухстороннего») безизбыточного выбора частоты дискретизации.

Анализ тенденций развития современной теории информации в условиях революционных изменений информационных технологий с терабитными возможностями вместе с тем указывает на необходимость концентрации усилий исследователей на вопросах её прикладной теории (профессор И.М. Коган), а также теории ценности информации (академик А.А. Харкевич), теории измерения её качества (квалиметрии) и полимодельного представления.

Это позволит, с одной стороны, усилить поиски путей и результативность минимизации избыточности обрабатываемых данных, как «вечной проблемы» теории информации. С другой стороны, станет возможным системно обоснованно и принципиально решать вопросы информационно-технического сопряжения психофизиологических возможностей операторов с возможностями современных информационно-управляющих систем при комплексной информационно-аналитической и интеллектуальной обработке данных, поступающих с мониторов эргатических комплексов и систем, а также - поддержке принятия управленческих решений. Это сегодня все более представляет проблему, требующую неотложного решения, в результате чего будет обеспечено информационно комфортное пространство управления все более сложными современными робототехническими системами.

Наконец, наряду с другими позитивными изменениями создание и интенсивное развитие теории управления информационным пространством позволит уже в ближайшей перспективе войти более подготовленными в полосу неминуемых широкомасштабных сетецентрических и информационных противоборств, что всегда оставалось и будет одной из ключевых национальных задач, а сегодня уже проявляется с особой силой в целом ряде направлений межгосударственных отношений.

Согонов С.А., Алексеев А.В., Тюрин И.С., Разживин Н.С., Жуланова Д.Н., Филиппова А.С., Шитикова К.А., Кальбфляш В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРЕДЛОЖЕНИЕ ПО СОЗДАНИЮ ПОЛИГОНА СЕТЕВОГО МЕЖВУЗОВСКОГО ВЗАИМОДЕЙСТВИЯ И МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Критический характер негативного влияния субъективных свойств персонала, так называемого пресловутого «человеческого фактора» (ЧФ) при управлении современными сложными информационно-коммуникационными и информационно-управляющими системами (ИС), необходимость совершен-ствования процессов управления информационным взаимодействием в организациях и в обществе в целом, создание и непрерывное совершенствование высоко-технологичных автоматизированных и автоматических комплексов и систем управления в информационно защищенном исполнении (АСЗИ) принципиально по-новому ставят вопрос и актуальную задачу моделирования процессов межсистемного и внутрисистемного взаимодействия, в том числе в части комплексного обеспечения безопасности.

Интенсивное развитие подсистем защиты информации в составе современных АСЗИ, их ключевое значение в составе современных систем обеспечения комплексной безопасности производственных комплексов и систем, социальных информационных сетей и систем и т.п. в сочетании с ограниченными возможностями использования только «оборонческих» технологий, необходимость их комплексного использования в сочетании с новыми технологиями активного информационного противодействия («наступательными» технологиями, технологиями сетецентрического противоборства) обуславливают острую необходимость создания и масштабной апробации многочисленных сегодня вариантов технологического развития методов обеспечения информационной безопасности (ИБ), информационного противодействия (ИПД) и в комплексе – информационного противоборства (ИП).

Существующих сегодня сетевых и организационно-технических ресурсов в организациях, участвующих в развитии технологий ИБ, ИПД и ИП, как правило, сегодня уже не хватает для отработки, освоения и внедрения новых информационно-технологических решений (ИТР) ИП, в том числе по причине различия, многообразия и динамического развития соответствующих научно-методических школ в данной новой предметной области с явно выраженным междисциплинарным характером. Это, как известно, сопровождается разобщенностью имеемых ресурсов и, даже, отставанием в развитии от международных (мировых) лидеров в области защиты данных, информационных сетей и жизненно важных, как следует из ФЗ «О безопасности», интересов личности, общества и государства.

В частности, с 2015 г. в Санкт-Петербургском государственном морском техническом университете в этой связи и контексте были разработаны концепция, положение и технология создания и развития Центра освоения технологий информационного противоборства и борьбы за информационную живучесть (БИЖ) объектов морской техники и морской инфраструктуры (сокращенно – ЦОТИП).

Целевая ориентация на совершенствование уровня подготовки и переподготовки обучаемых в СПбГМТУ был разработан и успешно проведен Весенний цикл тренингов по тематике ЦОТИП, наибольший интерес среди которых вызвали вопросы альтернативные архитектуры АСЗИ, мониторинг ИБ, ИПД и ИП, sniffing и spoofing, поиск и количественный анализ уязвимостей, ИБ систем массового спроса, технологии криптографии, алгоритмы стеганографии и соревнования CTF (capture the flag).

Ключевыми преимуществами подготовки слушателей ЦОТИП, как мы полагаем, явились и впредь будут культивироваться формирование устойчивых систематических знаний и владение практическими навыками обеспечения требуемого уровня качества АСЗИ и организационных мероприятий, направленных на повышение информационной защищенности ресурсов ОМТИ на основе своевременного освоения и эффективного использования комплекса технологий информационного противоборства.

В развитие сформированного подхода организационный комитет ЦОТИП и кафедра судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета предлагает расширить границы межвузовского взаимодействия в области ИБ, ИПД и ИП путем принятия концепции и создания Полигона сетевого межвузовскрого взаимодействия и моделирования процессов информационного противоборства (ПСМВ).

Основными задачами ПСМВ, по нашему мнению, должны быть:

– теоретическое обобщение и моделирование процессов ИП, их анализ, синтез и оптимизация, а также теоретическое обоснование практик создания, построения, освоения, эксплуатации и утилизации средств и технологий автоматизации процессов безопасной эксплуатации, локализации информационных инцидентов на объектах общего и специального назначения;

– освоение перспективных технологий ИП, обобщение и ранжирование лучших практик на основе систематизации данных и квалиметрического оценивания технологий ИБ, ИПД и комплексного ИП в целом в интересах ускоренного практического освоения и внедрения лучших проектных и управленческих решений в организациях и на предприятиях с учетом публикуемых данных;

– развитие и совершенствование практических навыков ИБ, ИПД и комплексного ИП студентов, магистрантов, аспирантов и преподавателей на основе проведения межвузовских сетевых тренингов практикующими специалистами смежных специализаций (администраторы ИБ, программисты, системные администраторы, специалисты по комплексной защите информации и т. п.);

– привлечение студентов к выполнению научных исследований на основе данных, получаемых в ЦОТИП (дампы трафики, новые сервисы и ПО, обнаружение новых векторов атак и т.п.);

– создание межвузовской технологической базы для сетевого взаимодействия и мониторинга состояния защищенности выделенных ресурсов, сегментов Интернета, а также моделирования и межвузовской тренажерной отработки технологий и задач ИП (сетецентрического противоборства, включая имитационное моделирование задач сетевых ИИ, атак, сражений, хаккинга и т.п.).

– формирование межвузовского научно-технического сообщества специалистов по ИБ, объединения их для решений сложных, наукоемких и ресурсоемких совместных проектов;

– разработка учебно-методических комплексов по технологиям ИП с формированием, ведением и актуализацией баз данных и знаний по технологиям ИБ, ИПД и комплексному ИП, а также лучшим практикам преподавания дисциплин по этим дисциплинам.

Создание ПСМВ позволит обеспечить в перспективе:

– организационно-техническое, научно-техническое и информационно-прозрачное пространство (площадку) для межвузовского взаимодействия при решении ресурсоемких и наукоемких современных проблем ИБ, ИПД и ИП в целом;

– регулярное проведение соревнований по ИП, например, в формате соревнований CTF, с целью повышения уровня квалификации участников взаимодействия, формирования региональной команды;

– межвузовскую научно-практическую лабораторию, центр, технопарк, позволяющие моделировать информационную модель города для практической отработки навыков атак и защиты.

Выступая с данным предложением, мы выражаем надежду на понимание и возможность практической консолидации усилий специалистов и профессионалов ВУЗов в области методов, технологий и средств обеспечения высокотехнологических решений обеспечения информационного противоборства, а также надежду на начало успешного и плодотворного содружества уже в ближайшее время.

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ЦОТИП В ВАРИАНТЕ "СПРУ-ИБ"

В условиях интенсивно развивающейся инфраструктуры систем защиты информации (СЗИ), а также все возрастающего числа проблем обработки информации и реагирования на всевозможные информационные инциденты остро встает вопрос о совершенствовании процессов и систем мониторинга, как средств автоматизации процессов наблюдения и соответствующей интеллектуальной поддержки принятия решений по получаемым результатам мониторинга.

В этой связи в СпбГМТУ в рамках выпускной квалификационной работы был создан программный комплекс макетного действующего образца (ПК МДО) системы поддержки принятия решений и управления «СПРУ-ИБ». Он был реализован путем адаптации базового ПК МДО по технологии систем поддержки принятия решений и управления «СПРУ» применительно к условиям решения задач ИБ и информационного противодействия (ИПД) в ранее созданном в СПбГМТУ Центре освоения технологий информационного противоборства (ЦОТИП) типовых объектов морской техники и морской инфраструктуры (ОМТИ).

При этом, были адаптированы структура, функциональный состав, информационное и программное обеспечение ПК МДО «СПРУ» с учетом специфических требований и решаемых задач администратором информационной безопасности ЦОТИП и решены следующие задачи:

Автоматической оценки качества, контроля и мониторинга ИБ и поддержки принятия решений Администратора ИБ (Аиб) ЦОТИП, что позволило свести к минимуму ряд ошибок управления ИБ, включая обусловленные негативным влиянием так называемого «человеческого фактора» (ЧФ).

Повышения оперативности (своевременности) принятия управленческих решений, что имеет особое значение для быстротечных процессов сетевого взаимодействия и больших объемов циркулирующей информации.

Мониторингу ИБ в последнее время уделяется все большее внимание. Уходят в прошлое предиктивные методы борьбы с информационными угрозами и все чаще при построении системы защиты информации стремятся делать акцент на мониторинге безопасности в реальном масштабе времени с эффективной поддержкой принятия решений АИБ. Причем, данные тенденции были отмечены и нашли свое отражение, например, в проекте Доктрины об информационной безопасности РФ (п. 29): «В рамках обеспечения функционирования системы информационной безопасности органы государственной власти решают следующие задачи: мониторинг и оценка состояния информационной безопасности Российской Федерации, прогнозирование и выявление источников угроз информационной безопасности, определение приоритетных направлений предотвращения и нейтрализации этих угроз; …».

СПРУ при качественном их проектировании и организации эксплуатации не должны «перегружать» оператора информацией, а создавать исключительно комфортную информационную обстановку для принятия оптимальных управленческих решений. При этом, все варианты решения возникшей ситуации должны быть обязательно сформированы в автоматическом режиме на основе базы данных и знаний, а также с учетом опыта предотвращения предыдущих подобных инцидентов. Именно такой подход (концепция) обеспечивают минимизацию негативного влияния субъективных (человеческих) факторов, что сегодня приобрело особое значение. И подобные СПРУ информационные технологии уже сегодня активно осваиваются в различных приложениях.

В процессе создания ПК МДО «СПРУ-ИБ» был произведен анализ уязвимостей, угроз и расчет рисков безопасности информационных ресурсов типовых ОМТИ. В докладе также представлен комплекс из 9 базовых (типовых) сценариев моделирования, апробации и технологической отработки порядка действий АИБ в условия информационного противоборства при проявлении различных информационных инцидентов. По результатам опытной отработки комплекса сценариев были получены следующие основные характеристики ПК МДО «СПРУ-ИП»: оперативность поддержки принятия решений и управления – от 2 минут; достоверность поддержки принятия решений и управления – порядка 85%; качество визуализации данных обстановки – более 95%; устойчивость поддержки принятия решений и управления – более 90%; скрытность поддержки принятия решений и управления – более 95%; непрерывность поддержки принятия решений и управления – более 95%; аппаратно-программные системные характеристики – не выше Pentium 4.

В результате выполненной работы был сделан вывод, что ПК МДО «СПРУ-ИБ» позволяет решать качественно новый ряд задач мониторинга ИБ в реальном масштабе времени. Это позволяет перейти от традиционного анализа данных по существу к автоматическому анализу и контролю самих процессов информационного противоборства с минимизацией потерь в контуре управления ИБ за счет негативного влияния субъективных свойств операторов ИБ.

Удодова Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРИМЕНЕНИЕ ОБОБЩЕННОГО МЕТОДА КВАЛИМЕТРИЧЕСКОГО АНАЛИЗА ПРИ ФОРМИРОВАНИИ СТРАТЕГИИ РАЗВИТИЯ ПРЕДПРИЯТИЯ

Современное состояние отечественного судостроения, как и других отраслей, характеризуется нарастающими темпами изменений во внешней среде (состояние экономики, санкции, катаклизмы, конкуренция, запросы потребителей, ускорение обновления применяемого оборудования, появление новых технологий, в т.ч. информационных, быстро меняющиеся ситуации и т.д.), которые, естественно, отражаются на состоянии (внутренней среде) организации.

Все эти факторы приводят к необходимости разработки руководством организаций долгосрочной стратегии развития, в которой должны предусматриваться, в том числе, меры по смягчению реакции на негативные воздействия внешней среды.

Выбор стратегии предполагает изучение альтернативных направлений развития организации, их оценку и выбор лучшей стратегической альтернативы для реализации. При этом используется специальный инструментарий, включающий количественные методы прогнозирования и разработку сценариев будущего развития.

Широкие возможности, по нашему мнению, в этом вопросе дает обобщенный метод квалиметрического анализа факторов развития (ОМКАР) для эргатических и эрготехнических (организационно-технических) систем (ЭТС).

Проведение многокритериального анализа системных свойств и характеристик предприятия, его конкурентной способности (КС) и перспективности развития (ПР) с использованием современных автоматизированных систем поддержки принятия проектных и управленческих решений (АСППР) на основе ОМКАР позволяет обоснованно переходить от факторного анализа к решению задач синтеза и оптимизации структуры и системных взаимосвязей предприятия при вариантном проектировании, а также обоснованно управлять его развитием.

Для создания системы поддержки принятия управленческих решений необходимо организовать структуру, которая среди прочих должна включать базу данных по экспертным оценкам, взвешенным с учетом индекса квалификации каждого эксперта, оценку частных показателей качества (ЧПК), групповых показателей качества (ГПК), агрегированных показателей качества (АПК). Подобные данные непрерывного мониторинга позволят оценить ПР и КС в процессе развития предприятия, наблюдать динамику изменения различных показателей качества и достаточно точно прогнозировать развитие текущих процессов. Это позволяет логически стройно и информационно прозрачно оценивать достигаемые при развитии предприятия результаты, оценивать ожидаемую эффективность соответствующих инвестиционных решений, а также квалиметрически прогнозировать качество ближайших, среднесрочных и дальнесрочных перспектив по достигаемым значениям АПК, ПР и КС предприятия.

С целью практической апробации и выявления специфических методических особенностей предложенного ОМКАР было выполнено численное моделирование с использованием фактических данных по реальному предприятию. В качестве объекта анализа было выбрано одно из ведущих научных предприятий отрасли, реализующих следующие направления деятельности:

- научно-исследовательские работы;
- опытно-конструкторские работы;
- научно-технические услуги;
- поставка судового оборудования и систем.

В процессе анализа с целью учета специфики данного предприятия была доработана предложенная ранее система критериев. Например, весомой оказалась такая техническая возможность внешней среды, как развитие компьютерного моделирования. Именно оно дает возможность сокращения дорогостоящих натурных экспериментов, что, в свою очередь, влияет на стоимость оказываемых предприятием услуг.

В докладе приведены данные ОМКАР–анализа данного предприятия, примеры оценок ЧПК, оказывающих существенное влияние на состояние предприятия, получены оценки АПК и ПР.

Анализ полученных оценок позволил определить факторы, оказывающие негативное влияние на развитие предприятия и сформировать рекомендации для их нейтрализации, а также определить факторы развития, обладающие наибольшим влиянием на величину прироста АПК и ПР.

Ушакова Н.П., Сус Г.Н., Алексеев А.В., Голубев И.Г, Москаленко В.А.
Россия, Санкт-Петербург, АО «Концерн «НПО «Аврора», Институт автоматизации процессов борьбы за живучесть корабля, судна

СИСТЕМНЫЕ ТРЕБОВАНИЯ И РАНЖИРОВАНИЕ КАЧЕСТВА ВАРИАНТОВ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ БЖКС

Одной из первостепенных задач развития интегрированных автоматизированных систем управления кораблем, судном сегодня является решение комплекса вопросов совершенствования автоматизированных систем информационно-аналитической и интеллектуальной поддержки принятия управленческих решений (СИП) с использованием всего спектра современных технологий.

Именно создание информационно комфортной обстановки для принятия результативных, эффективных и оптимальных, но, как правило, весьма сложных решений командиром корабля, капитаном судна и другими руководителями и начальниками, является ключевым элементом решения функциональных задач корабля, судна, а также обеспечения безопасности их эксплуатации, оперативной (своевременной) и эффективной локализации аварийных ситуаций и аварий, а также борьбы за живучесть корабля, судна (БЖКС). И в этом направлении сегодня достигнуты весьма значительные технологические и системные результаты.

Вместе с тем, интегрированная оценка, системный анализ и ранжирование проектного качества, эффективности функционирования, перспективности развития (ПР) и конкурентной способности (КС) подобных СИП является одной из традиционно сложных задач обеспечения управления развитием объектов морской техники. Это обусловлено рядом объективных и субъективных причин, включая: новизну направления; его бурное развитие; методическую сложность; наличие оператора в контуре управления (как наиболее критического и сложного для методического учета элемента управления); наличие у оператора известного негативного свойства – человеческого (ЧФ) фактора; традиционную «боязнь» количественных сравнительных оценок с конкурентами; стремление к использованию «упрощенных» схем обоснования; отсутствие опыта многокритериального оценивания качества.

Для решения этой актуальной проблемы предложены и обсуждаются системные требования и методический аппарат комплексного оценивания качества, КС и ПР СИП, включая комплекс критериев оценки и мониторинга качества СИП и управления БЖКС. Кроме того, приведены многочисленные практические пример оценки ряда вариантов построения и использования систем данного класса.

Впервые приведены методика и результаты решения оптимизационных задач вариантного выбора с использованием математического аппарата полимодельного квалиметрического анализа СИП БЖКС. На основе оценок элементов матрицы индексов критериальной чувствительности сформулированы предложения по приоритетному развитию альтернативных вариантов СИП путем наращивания/снижения значений соответствующих их системных и технических характеристик. Получены, представлены и обсуждаются соответствующие количественные оценки достигаемых (проектных) значений качества, перспективности развития и конкурентной способности СИП БЖКС.

При этом особое внимание уделено обоснованию предъявляемых к СИП требований и оценке возможности их реализации. Причем, как на этапе исследовательского и эскизно-технического проектирования, так и на этапах разработки конструкторской и технической документации, создания и всесторонних испытаний опытных и серийных образцов, их эксплуатации и модернизации.

Сформулированы и обоснованы научно-технические задачи дальнейшего развития представляемого методического аппарата оценки, системного анализа и ранжирования качества вариантов СИП и управления БЖКС, среди которых названы:

1. Систематизация данных в составе квалиметрических баз данных и знаний (КБДЗ) и сравнительный анализ конкурентной способности возможных методов и технологий реализации в составе интегрированных автоматизированных систем управления (ИАСУ) корабля, судна.
2. Разработка моделей и алгоритмов полимодельной оценки качества и эффективности функционирования перспективных СИП в составе ИАСУ корабля, судна с её объективной экспертной верификацией и оценкой валидности, например, в формате ранговой партнерской сертификации.
3. Разработка и аттестация программного комплекса полимодельной оценки качества и эффективности функционирования перспективных СИП в составе ИАСУ корабля, судна с адаптацией их к ряду типовых задач и к соответствующим моделям критериальных предпочтений.
4. Разработка и верификация комплекта (порядка 7) тестовых задач оценки качества и эффективности функционирования перспективных СИП в составе ИАСУ корабля, судна для сравнительного анализа и ранжирования используемых и новых методов и методик оценивания.
5. Проведение многовариантного численного эксперимента (моделирования качества) в интересах решения проектных оптимизационных задач в рамках исследовательского вариантного проектирования ИАСУ соответствующих проектов корабля, судна.
6. Решение оптимизационных системных задач для конкретных условий эксплуатации СИП в составе ИАСУ с экспертизой результатов и их аттестацией, а также актуализацией КБДЗ.
7. Создание КБДЗ по лучшим практикам построения и использования технологических решений в обеспечение СИП в составе ИАСУ корабля, судна, в том числе, например, в рамках проведения конкурсного сравнения перспективных технологических решений в формате «КСТР-2014», «КСТР-2016».

Ушакова Н.П., Москаленко В.А.
Россия, Санкт-Петербург, АО «Концерн «НПО «Аврора», ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»

МОДЕЛЬ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА СОВРЕМЕННЫХ КОРАБЛЕЙ

В докладе представлен анализ задач и проблем, которые необходимо решить разработчику при подготовке и разработке информационных технологий по обеспечению технического обслуживания кораблей с использованием современных требований. Определено, что внедрение информационных технологий, как правило, начинается с создания математического обеспечения, моделирования, формирования информационных хранилищ для промежуточных данных и решений. Рассмотрен порядок создания информационных технологий и определен путь решения.

При создании информационных технологий для обеспечения поддержки руководителей технического обслуживания кораблей и судов необходимо учитывать следующие ограничения и проблемы:

- существующие системы информационной поддержки не обеспечивают современных требований к обработке информации и времени на принятие решений;
- данная разработка не должна дублировать существующие системы;
- быть конкурентоспособной на мировом рынке;
- иметь возможность использования на судах и кораблях различных назначений и классов;
- разработка не должна противоречить принятым Руководствам и Положениям по техническому обслуживанию на кораблях и судах;
- разграничить возможности систем информационной поддержки при принятии управляющих воздействий на системы и выдачу рекомендаций лицу принимающему решение;
- тенденции современного развития систем безопасности непрерывно связаны с процессами широкой автоматизации и интеграции, которые не только касаются систем безопасности, но и всех остальных систем, предназначенных для управления техническими средствами.

Опыт, создания технологии систем информационной поддержки руководителей рассмотрен на примере создания СИП для кораблей и судов в рамках выполненных работ НПО «Аврора».

В НПО «Аврора» разработанная информационная технология – это совокупность средств и методов сбора, накопления, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или действия при решении задач.

Для командира ЭМБЧ разработана система информационной поддержки по организации эксплуатации технических средств и обучению личного состава.

Программа разработана в операционной среде “Windows”, с использованием приложения Microsoft Office “Access 2003”. Информационная часть программы использует приложения Microsoft Office «Word 2003” и “Excel 2003”

Разработанные информационные технологии – предназначены для рациональной организации процессов, протекающих в информационной сфере управления различными видами мероприятий на корабле и эксплуатации его технических средств.

Главная задача информационных технологий заключается в их целевой направленности на оптимизацию информационных процессов, т.е. процессов, выходным результатом которых является информация.

В качестве общего критерия эффективности информационных технологий использовался принцип сокращения времени на принятия решения, необходимого для реализации информационного процесса, организованного в соответствии с требованиями и рекомендациями этой технологии.

Критерий сокращения времени на принятия решения требует, в первую очередь, совершенствования наиболее массовых информационных процессов, оптимизация которых и должна дать наибольший выигрыш по этому критерию именно благодаря их широкому и многократному использованию.

Информационные технологии, разработанные в НПО «Аврора» имеют свои особенности:

1. Главная особенность - это информационных технологий в том, что поддержка принятия решений выходит на качественно новый метод организации взаимодействия человека и компьютера;

2. Выработка решения происходит в результате итерационного процесса, в котором участвуют:

а) система поддержки принятия решений в роли вычислительного звена и объекта управления;

б) лицо, принимающее решение, оценивающее полученный результат вычислений на компьютере;

4. Окончание итерационного процесса происходит по решению оператора; информационная технология поддержки принятия решений может использоваться на любом уровне управления.

В настоящее время существует необходимость разработки технологии, которая позволит освободить командиров боевых частей корабля от работы, связанной с накоплением информации о состоянии технических средств, подготовкой заявок на запасные части, составление ремонтных ведомостей для ремонта, сервисного обслуживания и работ, выполняемых личным составом. Сервисное обслуживание по решению командования ВМФ осуществляется комплексно по всем боевым частям и службам, в общем случае включает в себя:

а) работы, подлежащие обязательному выполнению независимо от фактического состояния корабельной техники;

б) авторский надзор, выполняемый ЦКБ - проектантами и проектантами основных составных частей (установок, комплексов, оборудования);

в) поставки ЗИП, материалов и комплектующих изделий в обеспечение эксплуатации кораблей;

г) работы по устранению эксплуатационных отказов и неисправностей.

При всех видах ремонта, переоборудования, модернизации, сервисного обслуживания документация (заявки на ремонт, ВРР, типовые ремонтные ведомости, заявки на ЗИП и оборудование и др.) оформляются личным составом кораблей и направляются головному исполнителю на электронных и бумажных носителях.

Алгоритм работы системы информационной поддержки состоит из:

- нормативных документов по стандартизации;
- нормативно - правовых актов федеральных органов исполнительной власти;
- эксплуатационных документов;
- комплекта документов для ремонта корабля;
- технологических документов;
- организационных и методических документов по мониторингу технического состояния корабля;
- отчетных документов, отражающих результаты мониторинга технического состояния корабля, ТД и НК;
- средств информационной поддержки жизненного цикла корабля.

Для создания автоматизированной системы для кораблей необходимо чтобы, электронная форма документов формировалась в едином программном продукте.

Под единым программным продуктом для ремонта, переоборудования, модернизации и сервисного обслуживания понимаются единая программа для ЭВМ и базы данных для программного обеспечения интегрированной логистической поддержки работ по сервисному обслуживанию и ремонту кораблей ВМФ, в рамках управления жизненным циклом кораблей ВМФ.

Система должна будет обеспечивать руководителей различных уровней:

- дорожными картами проведения работ с учетом времени и затрат на них;
- ремонтными ведомостями для различных организаций;
- заявками на запасные детали для организаций МТО;
- учет выполненных работ;
- и главное контролировать качество их выполнения.

Чернышев Д.Д., Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ ФИШИНГОВЫХ И АНТИФИШИНГОВЫХ ТЕХНОЛОГИЙ

Современные передовые технологии и, даже, в ряде случаев основы информационной безопасности известны отнюдь не каждому пользователю сетей. Этот факт очень часто ставит под угрозу безопасность самих сетей и конфиденциальность их информации.

Многие мошенники предпочитают использовать методику, работающую на незнании пользователями основ сетевой безопасности — фишинг. Это одна из разновидностей обмана пользователей, при котором поддельный сайт маскируют под совершенно обычную и знакомую пользователю точную копию окна авторизации какой-то сети. На поддельной версии объясняется причина повторной авторизации, и многие пользователи вводят там соответствующие данные, передавая их мошенникам. При помощи спам-технологий осуществляется рассылка пользователям сетей и жертвами таких обманов становятся многие.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Такие популярные браузеры как Internet Explorer, Opera, Safari, Firefox и др. уже обладают и по-своему широко используют такую возможность, которая соответственно получила название «антифишинг».

Антифишинг реализуется с помощью двух взаимодополняющих технологий. Первая – это встроенный в браузер плагин или антифишинговый фильтр, предупреждающий пользователя о попадании на подозрительный сайты. Вторая – это фильтрация фишинговых писем, рассылаемых злоумышленниками. Все подозрительные ссылки и вредоносные ПО хранятся в базе данных, которая находится в самом браузере, на компьютере или отдельном сервисе. При возможной атаке злоумышленника браузер исследует URL-строку, соединяется с базой данных и принимает решение по доступу пользователя к странице.

По статистике лаборатории NSS Labs только два широко распространенных браузера из 6 рассмотренных имеют процент отраженных атак свыше 80 процентов.

Кроме того, антифишинговые технологии также получили свое применение в антивирусных программах. Но и здесь следует учитывать, что не все из предложенных программ могут являться безопасными, т.к. за антивирусной программой может скрываться вирус.

На сегодняшний день проблема фишинга не решена в полной мере исключительно техническими средствами. Пока ведется поиск решения проблем и доработка существующих предложений, лучшей защитой от атак социальной инженерии злоумышленника, от загрузки вредоносного ПО является внимательность пользователей при работе в сети.

В докладе выполнен сравнительный анализ возможностей различных вариантов фишинговых и антифишинговых технологий и дан ряд практических рекомендаций пользователям по защите своих информационных ресурсов.

Филиппова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

К ВОПРОСУ О БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ МОРСКИМИ ОБЪЕКТАМИ

Современный уровень развития техносферы наряду с благами, принесенными Человечеству, создал новый, достаточно серьезный, вид угрозы – техногенные аварии и катастрофы, которые уже на протяжении 70-80 лет являются, как никогда, «непременными спутниками» технического прогресса.

Необходимость нейтрализации этой угрозы диктует необходимость наличия эффективного контроля и управления факторами опасностей, связанных, в том числе с функционированием

объектов морской техники и морской инфраструктуры (ОМТИ), создание и внедрение безопасных технологий эксплуатации и мониторинга безопасности ОМТИ.

Контроль технического состояния (ТС) и управление режимами работы ОМТИ осуществляется посредством автоматизированных систем управления технологическими процессами (АСУ ТП), которые делятся, как принято, на три уровня: нижний (представлен полевым оборудованием, исполнительными механизмами, датчиками), средний (программируемые логические контроллеры) и верхний (операторские и диспетчерские станции со средствами обеспечения принятия управленческих решений и их реализации).

Среди угроз безопасности АСУ ТП выделяют, как правило, три группы: угрозы техногенного характера, угрозы несанкционированного доступа и, к сожалению, пресловутый «человеческий фактор», поскольку управление ОМТИ традиционно является весьма сложным процессом, эффективность которого зависит не только от своевременности и достоверности полученной информации, но и от правильного ее восприятия и интерпретации операторами.

Повышению эффективности работы операторов и предотвращению возникновения аварийных ситуаций может способствовать внедрение в используемое программное обеспечение (ПО) новой опции прогнозирования, которая основана на однопараметрическом алгоритме.

Прогнозирование ТС ОМТИ является одной из задач технической диагностики, где под прогнозом понимается научно-обоснованное суждение и модель (физическая, математическая, алгоритмическая, вербальная и т.п.) о возможных состояниях объекта в будущем и (или) об альтернативных путях и сроках их достижения, а под прогнозированием – процесс разработки и использования модели прогнозов. К основным параметрам прогноза относят: период упреждения прогноза (промежуток времени от настоящего в будущее, на который разрабатывается прогноз); период основания прогноза (промежуток времени анализа предшествующих состояний, на базе которого строится история развития объекта прогнозирования с целью получения систематизированного описания модели априорной); достоверность прогноза (оценка вероятности осуществления прогноза для заданного интервала прогнозирования); ошибка (погрешность) прогноза (апостериорная величина отклонения прогноза от действительного состояния объекта прогноза).

В качестве исходного информационного массива ТС ОМТИ используется временной ряд (ВР) диагностического параметра, который представляется в виде аппроксимирующей функции - математической модели ВР. Однопараметрический алгоритм прогнозирования можно представить следующим образом.

Процедура диагностического мониторинга контролируемого параметра, в ходе которого формируется ВР с учетом некоторого количества ранее полученных данных.

Формирование базиса прогнозирования ВР при достижении некоторого значения диагностического параметра, одновременно производится оповещение оператора.

Аппроксимация полученного ВР с помощью операторов сглаживания, расчет коэффициента корреляции между исходным и сглаженным ВР.

Прогнозирование ТС. Доступ (отображение, визуализация) оператора к просмотру информационного сообщения о прогнозе и непосредственное его использование путем принятия соответствующих решений.

При получении предупредительного сообщения (при выходе процесса за допустимые границы) оператор должен оценить принятую информацию путем просмотра текущего состояния диагностируемых параметров в режиме реального времени, проверки и анализа истории значений, просмотра данных о прогнозе и принять соответствующие меры, например, заблаговременно подготовить технический персонал к предстоящим работам.

Таким образом, можно сделать вывод, что внедрение рассмотренного метода прогнозирования в АСУ ТП позволит повысить эффективность системы контроля и управления факторами опасностей, связанных с функционированием ОМТИ, и, как следствие, уменьшить вероятность возникновения аварийных ситуаций и, даже в ряде случаев, техногенных катастроф.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕТЕОРОЛОГИИ АРКТИЧЕСКОГО РЕГИОНА

Антонов К.В., Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОРГАНИЗАЦИЯ ПОДГОТОВКИ IT-СПЕЦИАЛИСТОВ ОСНОВАМ ЭКОЛОГИЧЕСКОЙ КУЛЬТУРЫ В АРКТИЧЕСКОМ РЕГИОНЕ

Важной составляющей программы является повышение экологической культуры населения, подготовка и повышение квалификации специалистов в области экологии. Наиболее развитым и доступным средством доставки оперативной информации является телевидение. Практически на всей территории России принимается телевизионные программы, которые формируются как центральными, так и региональными студиями.

В Санкт-Петербурге разработана однонаправленная система передачи компьютерной информации, которая использует в качестве носителя существующий аналоговый телевизионный сигнал передающих центров и не нуждается ни в телефонных линиях, ни в спутниковых «тарелках».

Техническая сущность предлагаемого решения состоит в том, что информационная посылка вписывается в телевизионный сюжет видеоряда и передается вместе с ним, причем содержание сюжета тематически связано с передаваемой информацией.

Далее видеосигнал вместе с дополнительной информацией, модулируется и в виде электромагнитных колебаний излучается в эфир.

На приемной стороне телевизионный сигнал, принимаемый обычной телевизионной антенной, поступает одновременно (параллельно) на антенный вход телевизора и на вход декодирующего устройства компьютера, которое устанавливается в свободный слот материнской платы.

В телевизионном приемнике происходит обычный процесс формирования изображения и звука, а в компьютере происходит выделение цифровой информационной посылки из аналогового видеосигнала и запись переданного информационного сообщения на жесткий диск, причем все это происходит в фоновом режиме. Объем передаваемой файловых посылок достаточно велик: за 10 минут вещания можно передать 2 - 4 мегабайт информации.

Передаваемый в составе видеосигнала цифровой поток обрабатывается помехозащищающими кодами (кодами Рида-Соломона), поэтому принимаемая информация имеет высокую достоверность. При необходимости, передаваемый цифровой поток может быть обработан кодами для криптозащиты.

Для оснащения системой ввода компьютерных файлов любого телевизионного центра не потребуется никакой доработки имеющейся аппаратуры формирования сигнала, т.е. предлагаемая система полностью вписывается существующей стандарт ТВ вещания России, стран СНГ и других европейских стран, вещающих в стандартах SECAM и PAL. Более того, образовательные программы могут поставляться на передающий центр на профессиональных стандартных кассетах формата Betacam SP, в которые уже вписана цифровая информация.

Что касается абонента, то ему достаточно иметь персональный компьютер (486 и выше) с установленной в нем платой декодирования, которая имеет свой адресный код. Стоимость платы декодирования – 50 – 70 €.

На основе этой системы передачи данных разработана новая технология дистанционного обучения. Достоинством такой технологии дистанционного обучения является сочетание огромного потенциала телевидения, его силу и глубину воздействия на зрителя, умноженного на серьезную самостоятельную работу на компьютере, анализ и поиск правильных решений, моделирование процесса, в результате чего слушатель осмысленно воспринимает изложенный материал, не абстрактно, а ассоциативно воспринимает факты и выводы.

Блочное построение учебных курсов позволяет осуществлять корректировку содержания предыдущих лекций этого курса при трансляции последующего материала, естественно, если в этом возникнет необходимость. Таким образом, учебный курс созданный в 2003 году и находящийся на сервере учебного заведения или в компьютере индивидуального пользователя может оперативно дополняться и исправляться при трансляции программ этого курса в последующие годы.

Описанная система по своим техническим возможностям может практически объединить существующие технологии дистанционного образования: портфельную, сетевую и телевизионно-спутниковую.

Система может быть использована также для передачи закрытой цифровой информации, для доступа к которой, абонент должен иметь соответствующий код идентификации, а для информации с криптозащитой - электронный ключ.

Описываемая техническое решение находится в стадии патентования (получена приоритетная справка и уведомление о положительном результате формальной экспертизы). Опытные экземпляры кодеров и декодеров прошли всесторонние испытания в НИИ Телевидения, телевизионный сигнал соответствует ГОСТу, гигиенические требования к аудиовизуальным параметрам ТВ сигнала одобрены специалистами Государственной технической комиссии при Президенте Российской Федерации.

При успешном испытании предлагаемой системы дистанционного обучения основам экологических знаний, она может быть рекомендована для внедрения на всей территории России.

Антонов К.В., Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ В АРКТИЧЕСКОМ РЕГИОНЕ

Практическая реализация экономического отторжения российских территорий может быть осуществлена с использованием проектов, направленных на интеграцию северо-западных субъектов Российской Федерации как сырьевых придатков в структуры Европейского союза.

В рамках этой интеграции:

создан Баренцево-Евро-Арктический регион, включающий в себя десять северных областей Швеции, Норвегии, Финляндии и России, в том числе Мурманскую и Архангельскую области и Республику Карелия;

с 1997 года осуществляется программа «Северное измерение» Президента Финляндии Пааво Липпонена, предусматривающая экономическое проникновение в Европейский Север России;

разрабатывается проект развития транспортной структуры «Северный коридор», реально позволяющей отрезать северные регионы от центра и включить их во внероссийское экономическое пространство;

разрабатывается проект интернационализации Северного морского пути (с учетом нарастающего старения российского атомного ледокольного флота, который в недалекой перспективе могут заменить корабли иностранных компаний);

активизированы международные отношения на региональном уровне для создания опоры на прозападно настроенные административные и деловые круги, компании и общественные организации, а также органы местного самоуправления с целью создания социальной базы поддержки.

Безусловно, что развитие международного сотрудничества на региональном уровне создает новые возможности для ускоренного формирования объединенного экономического пространства Российской Федерации и Европейского Союза.

В связи с реальной перспективой дальнейшего и увеличенного использования российских невозобновляемых сырьевых ресурсов в интересах глобальной экономики крайне необходимо, чтобы международное сотрудничество было выгодно в первую очередь России. Развитие перерабатывающих предприятий западных стран (наиболее активные из которых, принадлежащие Швеции, Финляндии и Норвегии), безусловно, должны обеспечивать развитие отечественного производства и, прежде всего, производство на Северо-западе России, предотвращая безработицу и развал экономики.

Геополитическая, социальная и экономическая ситуация на Севере России, возможные перспективы перехода северных областей под экономический контроль Норвегии, Швеции и Финляндии требуют разработки конкретных федеральных мер по защите государственных интересов Российской федерации, учитывающих активную и координированную политику Западных стран.

Информация о состоянии экосистем и антропогенных объектов - неотъемлемая составляющая при принятии экологических, оборонных и экономических решений.

Отсутствие необходимых данных о стихийных природных явлениях, о сложных гидрометеорологических явлениях и о загрязнения природной среды может иметь следствием человеческие жертвы, экологические катастрофы, экономический ущерб, ослабление вооруженных сил.

Следует отметить, что информация о состоянии природной среды и антропогенных объектов рассредоточена в различных ведомствах, взаимодействие которых не всегда осуществляется, в девяностые годы XX века в России значительно уменьшилось число пунктов наблюдения за окружающей средой.

С 1992 по 2001 годы количество пунктов наблюдения в Арктике сократилось более, чем на 25%, аэрологические наблюдения на обширных пространствах сокращены по сравнению с 1994 годом

почти в пять раз, северная морская гидрометеорологическая сеть сократилась более, чем на 40%. Достоверность прогнозов в значительной мере уменьшилась. Научно-исследовательский флот - морской компонент системы наблюдений переживает кризис. Количественный состав флота сократился, новые суда не вводятся в строй, приборная база не пополняется отечественным оборудованием. Океанографические экспедиции и экспедиции, связанные с разведкой и разработкой углеводородного сырья и добычей морепродуктов, приобрели чисто прикладную направленность. Российский научно-исследовательский флот перестает быть океанским, научные экспедиции - редкость.

Важная составляющая системы наблюдений – космические средства дистанционного зондирования в настоящее время недостаточно обеспечивают надежный спутниковый мониторинг Мирового океана. Для решения необходимых задач число космических средств должно быть, по меньшей мере, утроено.

Россия должна создать действенные федеральные структуры, способные надежно оценивать состояние природной среды и техногенных объектов, и разрабатывать планы их экологического оздоровления. В конечном итоге вопросы экологической безопасности России напрямую пересекаются с задачами обеспечения ее обороны. При анализе допустимых масштабов антропогенной нагрузки в Северо-Западном Федеральном округе должна учитываться и экологическая обстановка, причем не только в Баренцевом море, но и в других морях (как находящихся в пределах границ российского сектора Полярных владений, так и в сопредельных акваториях).

Бабкин Ю.А., Фёдоров А.В.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи

РАЗРАБОТКА КОМПЛЕКСА АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ИЗМЕРЕНИЙ И КОНТРОЛЯ ЛИНЕЙНОГО ТРАКТА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ МАГИСТРАЛЬНО-РАСПРЕДЕЛЕННОГО ТИПА С КОММУТАЦИЕЙ ОПТИЧЕСКИХ КАНАЛОВ СВЯЗИ

Согласно Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года предусматривается создание современной информационно-телекоммуникационной инфраструктуры в целях образования единого информационного пространства Российской Федерации.

Важным элементом создаваемой инфраструктуры должны стать магистральные сети связи, реализованные с применением подводных волоконно-оптических линий связи (ПВОЛС).

На всех этапах строительства, в процессе сборки и прокладки подводного кабеля, монтажа оборудования и эксплуатации необходимо применение оборудования, входящего в состав корабельного аппаратурно-кабельного комплекса, предназначенного для автоматизированного контроля оптических и электрических параметров ПВОЛС и управления измерениями.

В рамках проведенной ОКР специалистами Филиала ФГУП ЦНИИС – ЛО ЦНИИС был разработан взаимоувязанный комплекс аппаратных и программных средств (далее – комплекс), предназначенный для измерений и контроля оптических и электрических параметров линейного тракта (ЛТ) для ПВОЛС магистрально-распределенного типа с коммутацией оптических каналов связи.

Комплекс включает в себя:

1) средства измерений оптических параметров:
- анализатор оптического спектра FTP-5240SP;
- оптический рефлектометр FTP-7400E;
- измеритель хроматической дисперсии FTB-5800;
- измеритель поляризационной модовой дисперсии FTP-5500B;

2) Источник широкополосный оптического излучения FLS-5834A;

3) средства измерений электрических параметров:
- рефлектометр Teleflex SX;
- мегаомметр MIT525;
- миллиомметр МИКО-7;

4) автоматизированное рабочее место (АРМ);

5) оборудование коммутации пакетов информации К21;

6) систему гарантированного электропитания.

Все оборудование установлено в климатическом шкафу разработки Филиала ФГУП ЦНИИС – ЛО ЦНИИС.

Комплекс обеспечивает обнаружение и локализацию обнаруженных неисправностей ВОЛС, к которым можно отнести:
- обрывы кабеля;
- пробой изоляции;

– неисправности, вызванные выходом из строя компонентов ПВОЛС, некачественными сварными соединениями, увеличением потерь из-за попадания влаги в кабель, нарушением коммутаций в сети и др.

Комплекс предусматривает:

– измерение коэффициента затухания и вносимых потерь оптических волокон кабельных секций ЛТ с погрешностью не более 0,6 дБ на рабочей длине волны 1550 ±20 нм;

– измерение спектра оптического сигнала со спектральным уплотнением в контрольных точках ЛТ для анализа влияний нелинейных эффектов, измерение отношения сигнал/шум оптического сигнала со спектральным уплотнением, анализ неравномерности спектра пропускания оптического сигнала со спектральным уплотнением в линейном тракте в диапазоне длин волн 1525-1570 нм;

– измерение суммарного электрического сопротивления токопроводящей жилы кабеля с погрешностью не более 0,1 Ом/км;

– измерение электрического сопротивления изоляции токопроводящей жилы кабеля;

– измерение электрического сопротивления наружной оболочки кабеля;

– контроль электрического сопротивления изоляции токопроводящей жилы кабеля при технологических операциях с выключенным напряжением дистанционного питания;

– аварийную сигнализацию при любой нештатной ситуации;

– сбор и хранение данных на АРМ и внешних носителях с возможностью извлечения, корректирования, получения выборок, результатов сравнений и др.;

– передачу данных во внешние хранилища;

– архивирование результатов измерений в соответствии с регламентом.

Применение комплекса в составе двух современных кораблей-кабелеукладчиков («Волга» и «Вятка»), строительство которых ведется в России и планируется к вводу в строй в 2018–2019 гг. позволит активизировать работы по прокладке и расширению сети ПВОЛС в Арктической зоне Российской Федерации.

Ефимов В.В., Митько В.Б.
Россия, Санкт-Петербург, Ленинградское отделение Центральный научно-исследовательский институт связи

НЕКОТОРЫЕ ИТОГИ 4-Й КОНФЕРЕНЦИИ «СВЯЗЬ НА РУССКОМ СЕВЕРЕ»

IVконференция «Связь на Русском Севере – 2016»в этом году была проведена на юге России – в городе Сочи 15–16 сентября. Она была организована Издательским домом «Коннект» при поддержке Федерального агентства связи (Россвязь).Партнерами конференции в этом году выступили:ФГУП «Космическая связь» (генеральный партнер), «Корпорация «ТИРА», компания «Телекор» и ФГУП РТРС. Независимое издание PRO-ARCTIC являлось генеральным информационным партнером IVконференции, еще одним информационным партнером выступило агентство «Арктика-Инфо».

Развивая тему государственного подхода к проблемам развития связи на Севере РФ, Анатолий Брехунцов, генеральный директор НАО «СибНАЦ», председатель комиссии «Информационные системы и телекоммуникации» МОО «Ассоциация полярников»отметил, что сегодня горизонт проектирования в России, увы, ограничивается 2030 годом, в то время как для Арктики нужны проекты, рассчитанные до 50-х и даже 70-х годов. Валерий Митько, президент Арктической академии наук, отметил, что нам необходимо менять приоритеты, свое отношение к роли информационных технологий в экономике страны, поскольку уже сегодня стоимость интернет-трафика, который можно прокачивать по магистральным каналам связи из Китая в Европу,превышает доходы, которые мы извлекаем из перевозок грузов по Северному морскому пути.

Одним из путей устранения цифрового неравенства как признавалось в докладе Олега Ефремова, директора департамента ИТ и связи Ямало-Ненецкого автономного округа, является приоритетное направление именно прокладки линий ВОЛС, отметив ограниченность спутникового ресурса.

Далее, Илья Борисов, первый заместитель генерального директора ГУП «Технический центр телевидения и радиовещания» Республики Саха (Якутия) рассказал о роли региональных операторов связи в развитии коммуникационной отрасли Республики Саха (Якутия).

В течение первого дня работы форума также прозвучали выступления представителей нашей космической отрасли – ФГУП «Космическая связь» и АО «Информационные спутниковые системы» им. академика М.Ф. Решетнева рассказали о текущих проектах и представили перспективные системы связи для территории Крайнего Севера и Арктики.

После выступления нескольких докладчиков, которые подняли тему развития радиосвязи на Русском Севере, в аудитории вспыхнула незапланированная дискуссия, в ходе которой участники форума смогли высказать свои зачастую диаметрально противоположные позиции. Тем не менее, в

конечном итоге, после довольно бурного обсуждения им удалось достигнуть взаимопонимания по некоторым принципиальным вопросам.

На пленарном заседании можно отметить выступление Станислава Кузнецова, директора филиала РТРС «Дальневосточный РЦ»:он обратился к участникам президиума с настоятельной просьбой взять под свой контроль дальнейшую координацию работы участников форума, чтобы общими усилиями привлечь внимание к проблемам связи на Русском Севере и найти возможности для реального изменения ситуации к лучшему.

Второй день работы конференции открылся докладом старшего научного сотрудника НИИ оперативно-стратегических исследований строительства ВМФ ВУНЦ ВМФ «ВМА» Вячеслава Цыванюка. Его выступление было посвящено перспективам развития системы связи ВМФв АЗРФ. Вячеслав Цыванюк указал на тот факт, что сеть подводных ВОЛС в Арктике развита недостаточна, однако в скором времени ситуация изменится – в России сейчас ведется строительство двух современных кораблей-кабелеукладчиков («Волга» и «Вятка»), которые войдут в строй в 2018–2019 гг.

Александр Лабардин, начальник федерального учреждения «Арктический спасательный учебно-научный центр «Вытегра», рассказал об особенностях использования средств связи в длительных автономных экспедициях в Арктике. В своем выступлении он, в частности, отметил, что система связи «Гонец» на базе низкоорбитальных спутников не устраивает полярников, поскольку она не обеспечивает устойчивую связь на высоких широтах, в результате участники экспедиций работают на системе Iridium.

О непростых проблемах, стоящих перед «Росгидрометом», участникам форума поведал Александр Кузьмичев, главный специалист отдела совершенствования ледовой информационной системы ФБГУ «Арктический и антарктический научно-исследовательский институт» Росгидромета. Так, он подчеркнул, что болевой точкой для метеорологов Арктики сегодня является отсутствие российских спутников, которые могли бы предоставлять фотографии высокого разрешения, необходимые для прогнозирования ледовой обстановки Северного морского пути. Стоимость одного снимка с зарубежного спутника составляет в среднем порядка 3000 долларов США. В качестве решения этой проблемы Александр Кузьмичев предложил использовать БПЛА. Большое место в своем докладе представитель «Росгидромета» также уделил необходимости развития сети КВ радиосвязи в районах Крайнего Севера и Арктики.

После этих «проблемных» докладов, вызвавших живое обсуждение участников форума, хорошей порцией оптимизма с делегатами конференции поделился Михаил Смычек, главный специалист отдела проектирования сетей связи АО «Гипрогазцентр». В своем докладе он высказал довольно спорные суждения, например, о том, что будущее связи только за ВОЛС. Несколько участников форума немедленно выступили в защиту радиосвязи и спутникового сегмента. В завершающей части пленарного заседания прозвучали целых три доклада по несколько непривычной для российского ИТ-сообщества тематике, которая была отмечена и на прошлых конференциях «Связь на Русском Севере», а именно: «телекоммуникационные технологии на службе медицины». Один из постоянных участников форума «Связь на Русском Севере» Светлана Мананкова, старший советник Центра развития и качества Университетской больницы Северной Норвегии, рассказала о том, как в течение 25 лет развивалась отрасль телемедицины в Норвегии. При этом она особо подчеркнула, что одним из главных факторов успешного развития здесь была личная инициатива неравнодушных людей – медиков и ИТ-специалистов. Затем с кратким, но весьма содержательным докладом выступил Игорь Шилкин, начальник Центра управления в кризисных ситуациях Штаба Всероссийской службы медицинских катастроф. Докладчик представил первые итоги создания единого информационного пространства для развития услуг телемедицины в АЗРФ.

Завершающим докладом по медицинской тематике стало выступление Артема Андреева, адъюнкта при НИО НИЦ Военно-медицинской академии им. С.М. Кирова. Оно было посвящено инновационным технологиям для оказания медицинской помощи. Честно признаемся, было приятно узнать, что российские военные медики, как говорится, «держат руку на пульсе» – подполковник Андреев рассказывал о необходимости внедрения таких современных устройств, как «умные часы» (измерение пульса, расстояния), «умные очки» (для людей с болезнью Паркинсона), всевозможные трекеры, медицинские трикодеры, «умные контактные линзы», пилюли со встроенной камерой. Закончил свое выступление Артем Андреев отчетом о создании опытной зоны для испытания телемедицинских технологий на уровне медицинская рота – войсковой госпиталь – центральный госпиталь.

Поэтому совсем не случайно заместитель генерального директора РТРС Виктор Горегляд, подводя итоги «круглого стола», посвященного проблемам развития радиовещания на Крайнем Севере, призвал участников конференции делать ставку на развитие региональных инициатив, не дожидаясь того, когда их проблемы придут решать чиновники из Москвы.

Участники конференции положительно отнеслись к предложениям ЛО ЦНИИС и созданию на его базе Инновационного центра инфокоммуникационных технологий, выражая готовность к сотрудничеству по созданию единой инфокоммуникационной системы России в Арктике.

Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСОБЕННОСТИ «ГИБРИДНЫХ ВОЙН» В АРКТИЧЕСКОМ РЕГИОНЕ

Страны, претендующие на господство в Арктическом регионе, все чаще используют в понимании современных методов ведения противоборств – противостояния термин «гибридной войны».

Гибридная война (англ. hybrid warfare) – термин, появившийся в конце XX века в США для понимания военной стратегии, объединяющей в себе как единое целое обычную войну и информационную войну. Следует подчеркнуть, что в мире пока нет единого и общепринятого определения. Само слово «гибридный» означает использование сразу нескольких видов давления (информационно-идеологическое, финансово-экономическое и т.д.) на противника. При этом действия вооруженных сил составляют хотя и важную, но всего лишь часть.

Важными инструментами в практике ведения гибридных войн являются:

- информационные операции, проводимые в целях воздействия на органы государственного и военного управления противника для введения его в заблуждение, нарушения обмена данными и провоцирования на принятие выгодных для него решений;
- психологические операции, направленные на подавление морально-психологического состояния населения и боевого духа личного состава вооружённых сил противника, создание в обществе атмосферы недоверия и формирование мотивации к деструктивным действиям;
- кибернетические атаки на государственную и коммерческую инфраструктуры с целью выведения из строя или затруднения работы критически важных объектов противника, а также получения несанкционированного доступа к «чувствительной» информации;
- экономические санкции, прекращение инвестиций;
- этническое оружие;
- организационная, финансовая и информационная поддержка оппозиционных движений, деструктивные действия «агентов влияния», внедренных в структуры власти. Основными принципами ведения гибридной войны являются стратегическое планирование, координация, взаимодействие, своевременность, внезапность и скрытность.

Противостояние «гибридной войне» является актуальной темой различных конференций и круглых столов, в ходе которых выдвигаются различные предложения по противодействию гибридным войнам. Так, на данный момент предложено создание своих собственных информационных пропагандистских структур, ориентированных на конкретную аудиторию населения, создание научных организаций, которые будут разрабатывать технологии противодействия враждебной пропаганде в обществе с использованием современных информационных технологий. Одной из мер противодействия может выступить укрепление экономики, повышение уровня жизни в стране, а также устранение явных проблем государства, которые могли бы вызвать недовольства граждан страны.

Первые информационные войны вокруг Арктики начались еще в 2006 году. Одной из целей, которых является объявить мировому сообществу о неспособности российских грузоперевозчиков достойно конкурировать с компаниями Западной Европы.

Однако, очевидно, что сегодня, мало просто заявить о своих политических правах на территории и морские трассы, необходимо обладать современными знаниями и технологиями освоения богатств Арктики, развития транспортных магистралей. Достойным ответом на информационные атаки зарубежных конкурентов должны стать меры поддержки научных исследований и технологий хозяйственной деятельности в экстремальных для человека условиях. Кроме того, в соответствии с «Основами государственной политики в Арктике...», Россия приступила к размещению военного контингента в Арктическом регионе. Предполагается, что основные силы будут размещены на архипелаге Земля Франца-Иосифа, которому в 90-е годы наши «северные» соседи пытались предать международный статус.

Гибридные войны невозможно увидеть закрепленными юридически, как правило, они происходят негласно. Актуальной задачей любой из стран противостоять данной войне, готовить свою страну к возможной гибридной угрозе со стороны государства агрессора..

Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРИМЕНЕНИЕ ДИФФУЗНЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В АРКТИЧЕСКОМ РЕГИОНЕ

Одно из примечательных явлений в науке заключается в стремлении перейти от изучения хорошо организуемых систем к плохо организуемым, или диффузным системам.

Диффузные геоинформационные системы (далее система) — это системы, в которых нельзя «установить непроницаемые перегородки», разграничивающие действия или явления переноса

влияния переменных различной природы. Этими принципиальными особенностями диффузные системы выделены в класс сложных систем. Разнообразие ГИС допускает существование как хорошо организуемых, так и диффузных систем.

Системы управления и основные её составляющие, по своей природе — диффузные системы, так как любое принимаемое решение, согласно закону о динамическом равновесии, некоторым неизвестным образом отразится на результатах процессов или действиях элементов системы управления. Если мы говорим о хорошо организуемых системах, то это или системы с замкнутым контуром и управлением по отклонениям, или самонастраивающиеся системы, способные выдерживать воздействие внешней среды за счет способности к адаптации. В системе с замкнутым контуром в процессе управления все время осуществляется обратная связь в целях минимизации возникшего отклонения.

Самонастраивающаяся система — это система, способная обеспечить устойчивое функционирование организации в условиях произвольно возникающих и изменяющихся возмущающих воздействий внутренней и внешней среды. Система реализует два контура управления — управление по отклонениям и управление с адаптацией путем введения в систему компенсационных элементов, например запасов сырья, резервных мощностей и др. Термин «самонастраивающаяся система» является синонимом термина «адаптивная система». В класс самонастраивающихся включаются и системы, о которых известно, что их динамические параметры будут претерпевать изменения. Это явление закономерно для развивающихся организационных систем. В зависимости от сложности таких систем, управление ими может осуществляться по принципу хорошо организуемых систем или диффузных систем.

Систему, способную за счет изменения своих свойств сохранять устойчивый характер взаимодействия с внешней средой, несмотря на возможные изменения внешних и внутренних факторов, называют самоорганизующейся.

Принятие модели системы как диффузной вместо хорошо организуемой, равновесной системы повлекло за собой изменения в методологии и теории исследований систем управления.

Математические модели преобразования входных ресурсов и модели, описывающие связи между входными ресурсами и выходными результатами, отличаются значительным разнообразием. Это могут быть модели, основанные на идеях и методах многомерной математической статистики, методах исследования операций, математической логике и т.д.

Диффузная система как любая сложная система должна поддерживать свои параметры и функции в определенном диапазоне на основе создания устойчивой внутренней среды относительно возмущающих воздействий внешней среды и происходящих случайных «отказов» в ней самой, т.е. создавать свой гомеостаз, определенную форму устойчивого функционирования за счет адаптации и гибкости.

На современном этапе в теории управления система отождествляется с организмом, а организм означает систему, имеющую свои собственные цели, рожденные ее внутренней сущностью с возможностью им следовать. Цель развития такой системы — это новый гомеостаз. Этим понятием определяется «согласованная с состоянием Природы и ее законами» форма развития системы, которая рассматривается как «устойчивое неравновесие» (sustainability development).

Применительно к исследованию систем управления понятие формы развития системы как «устойчивого неравновесия» наглядно подтверждается закономерностью жизненного цикла системы. Гомеостаз — многопараметрическое пространство, в котором, несмотря на некоторую флуктуацию системы, обеспечивается ее равновесие.

Диффузная система должна обладать свойством самоорганизации, подразумевающей прежде всего способность к самообучению, выбору вариантов и механизмов их отбора, что обеспечит ее развитие, а далее — адаптацию к условиям существования. Механизм самоорганизации может развиваться только в системах, характеризующихся «принципиальной стохастичностью» и «принципиальной неустойчивостью».

Диффузные системы — это открытые системы, которые обмениваются энергией (результатами работы) или информацией с внешней средой. Главенствующую роль во внешней среде системы играют не порядок, стабильность и равновесие, а неустойчивость и неравномерность. Это объясняется тем, что все системы непрестанно флуктуируют. В особой точке бифуркации флуктуации достигают такой силы, что система не выдерживает и разрушается, которые называют диссипативной структурой. Диссипативные структуры существуют лишь тогда, когда система диссипирует (рассеивает) энергию, в результате чего возникает порядок.

Примером диссипативных структур служат сетевые организационные структуры. На практике диффузия и флуктуация системы несколько приглушаются рассеиванием энергии более мощной системы в виде создания сетевых структур. Современная концепция ведения сетецентрических «гибридных войн» в Арктике обуславливает очень жесткие требования к оперативности и живучести управления на базе сетевых технологий. Геоинформационные диффузные системы позволяют вывести эти качества на новый уровень.

Митько В.Б.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи

СТРАТЕГИЧЕСКОЕ ЗНАЧЕНИЕ ФОРМИРОВАНИЯ ЕДИНОЙ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ АРКТИЧЕСКИХ РЕГИОНОВ

Прежде всего целесообразно обратиться к глобальным противоречиям XXI века и определиться с тезисом «уменьшают или усугубляют их арктические перспективы».

Среди глобальных проблем современности, как совокупности социально-природных проблем, от решения которых зависит социальный прогресс человечества и сохранение цивилизации, можно указать на следующие:.

- проблема «Север-Юг» - разрыв в развитии между богатыми и бедными странами, нищета, голод и неграмотность;
- социальное неравенство - разрыв между 1 % самых богатых и остальным человечеством
- угроза термоядерной войны и обеспечение мира для всех народов;
- катастрофическое загрязнение окружающей среды;
- снижение биоразнообразия;
- обеспечение человечества ресурсами, исчерпание нефти, природного газа, угля, пресной воды, древесины, цветных металлов;
- демографическое развитие (демографический взрыв в развивающихся странах и демографический кризис в развитых), возможный голод.

Даже неглубокий экспертный анализ ставит под сомнение тезис о том, что арктические перспективы не усугубляют эти глобальные противоречия, а одним из направлений, смягчающих эти противоречия, является развитие транспортно-коммуникационных и инфо-коммуникационных систем.

Применительно к регионам АЗРФ основными геополитическими преимуществами являются:

- обеспечение транспортного и информационного суверенитета в Арктической зоне Российской Федерации, организация связи и управления – фундамента Центра управления АЗРФ;
- снижение риска препятствий устойчивому развитию региона;
- гарантированное достижение глобально-регионального баланса в регионе для достижения национальной и региональной безопасности (недопущения распада);
- более чёткие контуры прогнозирования сценариев регионального и глобального развития;
- возрастание значения интеллектуального фактора-одного из определяющих в 21 веке.

Основные экономические преимущества:

- обеспечение более эффективного пространственного планирования и научно обоснованного распределения территорий опережающего развития;
- возможности применения научно обоснованных проектов и программ вместо ведомственно-ориентированных;
- достижение наиболее рационального распределения инвестиционных усилий в регионе;
- более реальные прогнозы социально-экономического развития (отсутствие ангажированности, конкурентной коньюнктуры и неизбежность ответственности за качество (объективность) прогнозирования;
- обеспечивается взаимодополняемость возможностей различных составляющих системы (по исследованиям китайских коллег);
- развитие технологий различных стран в инновационном направлении;
- более рациональное распределение инвестиций при наличии и проявлении политической воли органа управления.

Основными негативными сторонами возможностей развития единой инфокоммуникационной системы арктических регионов являются трудности реализации политической воли в координации и гармонизации элементов системы управления хозяйственной и иной деятельности, необходимость унификации, стандартизации, согласования и координации деятельности различных ведомств и государств.

Особенности построения инфокоммуникационных сетей в Арктическом регионе определяются:

- низкой плотностью хозяйственной инфраструктуры и населенности в районах Крайнего Севера и Дальнего Востока;
- высокой стоимостью строительства линейных сооружений и узлов связи;
- исключительной сложностью эксплуатации объектов связи в арктических географических условиях;
- особенностями использования различных сетей связи в условиях Арктики;:
- ведущей ролью подводных кабельных магистралей в построении опорной сети связи по арктическому побережью;
- недостаточной эффективностью применения геостационарных спутников для связи в высокоширотных районах;

– низкой рентабельностью сотовых сетей связи в районах с низкой плотностью населения;
– сложностью построения прямых магистральных коротковолновых линий связи из-за особенностей распространения радиоволн в регионе.

В Ленинградском отделении ЦНИИ связи разработаны предложения по построению магистральных сетей связи в АЗРФ, основанные на волоконно-оптических кабельных системах.

Основными преимуществами подобной структуры являются:
– повышение устойчивости системы управления;
– укрепление национальной безопасности в Арктике;
– обеспечение импортозамещения при производстве и эксплуатации.

Этот далеко не полный перечень можно резюмировать, как формирование материально-информационного каркаса страны в системе глобальных тенденций мирового развития.

Митько В.Б., Минина М.В.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи, Арктическая общественная академия наук

СОЗДАНИЕ ИННОВАЦИОННОГО ЦЕНТРА АРКТИЧЕСКИХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЛО ЦНИИС

Инновационный центр Арктических инфокоммуникационных технологий создан в соответствии с Приказом президента Санкт-Петербургской научной общественной организации «Арктическая общественная академия наук» (СПб НОО АОАН) и Соглашением между Санкт-Петербургской научной общественной организацией «Арктическая общественная академия наук» и Ленинградским отделением Центрального научно-исследовательского института связи (ЛО ЦНИИС) в целях выполнения Федеральных целевых программ, приоритетных направлений развития науки, технологий и техники РФ и ведомственных программ Рособрнауки и других министерств и ведомств, а также научных и образовательных процессов с широким привлечением молодых ученых, аспирантов и студенческой молодежи для реализации научного направления «Арктические инфокоммуникационные технологии». Предполагается развивать на его основе формирование кластера инфокоммуникационных технологий, составляющего основу формирования единой евразийской системы.

Центр формируется на базе секций «Геополитики и безопасности» и «Информационных технологий» АОАН и лабораторий ЛО ЦНИИС и является структурным подразделением АОАН, он осуществляет научно-исследовательскую, научно-образовательную, информационно-методическую и инновационную деятельность, обеспечивает координацию работ по направлению «Арктические инфокоммуникационные технологии».

Основной целью создания центра является:
– реализация научных исследований и разработок в области арктических инфокоммуникационных технологий;
– проведение теоретических, натурных и лабораторных исследований методов и средств арктических телекоммуникационных технологий;
– осуществление математического и имитационного моделирования и развития методов защиты информации, оперативной оценки защищённости телекоммуникационных систем;
– обработки информации, разработки алгоритмов и программного обеспечения в системах защиты информации;
– обеспечение образовательной деятельности в области подготовки и переподготовки кадров, включая подготовку бакалавров, специалистов, магистров, кандидатов и докторов наук по инфокоммуникационным специальностям;
– обеспечение взаимодействия с академическим и отраслевым секторами науки для повышения эффективности научно-исследовательской и научно-образовательной деятельности;
– участие в разработке программ обучения, и популяризации знаний в сфере арктических инфокоммуникационных технологий, информационной безопасности для формирования новой технологической культуры.

Поставленная цель достигается путём решения следующих основных задач:
– развития материально-технической базы научного-исследовательского и образовательного процессов;
– организации на базе центра научных исследований, развития технологий, образовательного процесса;
– интеграции и координации научно-исследовательской и образовательной деятельности в рамках реализации процесса повышения квалификации научных и инженерных работников, профессорско- преподавательского состава а также представителей сторонних предприятий и организаций;
– широкого привлечения преподавателей, научных работников, инженеров, аспирантов и студентов планируемого к формированию консорциума (кластера) к НИОКР по фундаментальным и

прикладным проблемам арктических инфокоммуникационных технологий и информационной безопасности;

– развития стратегического, научного и международного партнерства.

Основными функциями центра являются:

– кадровое, материально-техническое и информационно-методическое обеспечение научно-исследовательского и образовательного процесса в соответствии с образовательными стандартами по актуальным направлениям и профилям подготовки бакалавров, магистров и аспирантов;

– развитие и проведение фундаментальных и прикладных НИР и НИОКР;

– обеспечение взаимодействия фундаментальной и прикладной науки с образовательным процессом профильных вузов на всех его стадиях, включая коммерческое использование результатов совместных научно-исследовательских и опытно- конструкторских работ;

– обеспечение процесса переподготовки кадров для отрасли в тесном взаимодействии с государственными учреждениями и научными организациями Минобрнауки и других ведомств;

– организация эффективного взаимодействия с другими центрами научных организаций и вузов для совместной разработки арктических технологий нового поколения, реализации качественного обучения по программам специализированной магистерской подготовки в области инфокоммуникационных систем и информационной безопасности.

– осуществление международного сотрудничества путём выполнения научных контрактов, участия сотрудников центра в работе международных конференций, международного обмена сотрудниками и молодыми учёными.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИЗДАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ, ПОЛИГРАФИИ И ДИЗАЙНЕ

Ардашева А.О., Тропец В.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ПРИМЕНЕНИЕ КОНЦЕПЦИИ ПРОЦЕССНОГО ПОДХОДА ДЛЯ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ В ТИПОГРАФИИ

Эффективное управление производственными процессами предприятия позволяет снизить затраты на изготовление продукции, повысить ее качество, оптимизировать использование ресурсов и увеличить прибыль. В связи с этим все большее распространение получают системы управления процессами. В практике крупных компаний принято, что проектами по разработке и внедрению таких систем занимается IT-служба. Специалисты данного подразделения хорошо знакомы с технологией моделирования, а оперативное внутрифирменное взаимодействие позволяет добиться положительных результатов. Но, к сожалению, немногие типографии обладают такими кадровыми ресурсами.

Средние и малые организации, как правило, прибегают к использованию типовых программных продуктов, представленных на рынке в широком ассортименте, а также привлекают сторонних специалистов для проектирования систем. Однако, в данном случае, предприятие чаще всего сталкивается с тем, что система оторвана от реальной деятельности и получается, что технологические процессы не нуждаются в совершенствовании, персонал обучается сам собой, а брак отсутствует. Но прибыль и удовлетворенность потребителя почему-то не увеличиваются. Надо понимать, что, во-первых, ни одна типовая система не учитывает особенностей процессов, происходящих на конкретном предприятии, а, во-вторых, незнание современных принципов управления сотрудниками компании на разных уровнях не дает возможности эффективного использования данных программных продуктов, ведь, в конечном счете, управляющее решение принимает человек, а не программа. На основе анализа литературных источников и практики различных компаний можно предположить, что базисом эффективного управления процессами являются понимание руководителями и рядовыми сотрудниками компании деталей собственных процессов и применение к ним современных принципов управления, в частности, процессного подхода. В таком случае, разработанный или приобретенный программный продукт будет эффективным инструментом для решения поставленных задач.

Целью работы являлась оптимизация производственных процессов типографии «МДМ-печать». Для достижения поставленной цели необходимо было выбрать наиболее эффективные методики моделирования и анализа процессов производства продукции, методы оценки и снижения риска возникновения несоответствий, разработки механизмов совершенствования процессов.

На первом этапе процессы были классифицированы по принципу «процессы, добавляющие ценность» и «процессы, добавляющие стоимость». Данная, достаточно условная, классификация позволяет провести подробный анализ и декомпозицию процессов предприятия. Сложная траектория реального рабочего потока в значительной мере увеличивала время выполнения работ и требовала пересмотра взаимодействия между подразделениями. Также анализ показал низкий уровень документированности основных процессов и отсутствие показателей эффективности и результативности их выполнения. Делегирование полномочий подчиненным и распределение ответственности также требовали пересмотра. Полученные сведения позволили определить проблемные узлы процесса производства продукции, выделить операции, требующие автоматизации, а также составить техническое задание на разработку системы управления процессами, так как программные продукты, представленные на рынке, не в полной мере удовлетворяли установленным требованиям.

Далее, для снижения риска возникновения несоответствий при производстве продукции, были проанализированы виды брака и его количество за последние 5 лет. Было установлено, что больше всего претензий приходится на операции с низким уровнем регламентации процесса. Среди основных причин возникновения несоответствий отмечены халатность сотрудников, а также сложности во взаимодействии между подразделениями. На основе полученных данных и интервьюирования сотрудников предприятия была проведена идентификация и оценка степени риска на основных процессах. С применением стандарта ГОСТ Р ИСО/МЭК 31010-2011 были разработаны процедуры, целью которых являлась минимизация возникновения несоответствий.

По результатам проведенного исследования можно сделать вывод, что для внедрения процессного подхода в типографию необходимы: четкое понимание целей проекта по описанию процессов предприятия, обучение сотрудников всех подразделений, командная работа и заинтересованность руководителей.

Архипов П.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна

АНАЛИЗ ЭФФЕКТИВНОСТИ ИНТЕРНЕТ-КАНАЛОВ ПРИВЛЕЧЕНИЯ ТРАФИКА

Постоянный анализ и подбор интернет-каналов – неотъемлемая часть любой контент-маркетинговой стратегии. Довольно сложно определить четкий алгоритм определения эффективности рекламы в сети Internet. Основная сложность заключается в разновидности сайтов и их целей, а так же возможностей продвижения сайтов и товаров.

Сайты можно разделить на два типа информационные и продающие, а, следовательно, и продвижение этих сайтов можно поделить на поиск пользователей и поиск покупателей. Каналы для привлечения пользователей и покупателей различаются, хотя некоторые подходят как для одних, так и для других.

Существует множество способов привлечения трафика. Основные из них – это SEO оптимизация, SMM, контекстная реклама, тизерные сети, CPA-сети, Google.Adwords, Яндекс.Директ, реклама на Youtube, различное продвижение в социальных сетях (VK, Facebook, Instagram, Одноклассники) и спам.

Определить какой из рекламных каналов работает лучше всего для конкретного сайта необходимо, чтобы минимизировать затраты владельца сайта и увеличить конверсию через этот канал. Для этого необходимо протестировать основные каналы продвижения, которые являются наиболее подходящими по типу для рекламируемого сайта. Сбор данных о посещаемости и целевых действиях пользователей дает возможность подобрать такие каналы, которые будут эффективны для каждого конкретного случая.

Галимова Е.Ю.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

АНАЛИЗ ПОДХОДА К ТЕСТИРОВАНИЮ ПРОГРАММНОЙ СИСТЕМЫ НА БАЗЕ РЕШЕНИЯ МНОГОКРИТЕРИАЛЬНОЙ ЗАДАЧИ

Любая программная система включает в себя в первую очередь набор программного обеспечения (ПО) и, в некоторых случаях, компьютерное оборудование, обеспечивающее функционирование ПО. Требования к качеству ПО регулярно возрастают. Рассматриваемый в данной работе подход к оценке качества ПО реализовывался в рамках каскадной модели разработки программного продукта (ПП). Он базируется на следующих характеристиках ПП, определяющих его полезность для потенциальных пользователей: функциональные возможности, надежность, практичность, эффективность, сопровождаемость, мобильность.

Жизненный цикл ПП в рамках каскадной модели включает четыре этапа: подготовка, разработка, тестирование, внедрение. Перед началом этапа тестирования, для корректировки и усовершенствования тест – плана, предлагается выдавать группе разработчиков опросный лист, каждый вопрос в котором отражает определенные свойства ПП. Заполненные разработчиками опросные листы поступают в отдел тестирования. Оценки в этих листах имеют бинарный вид: «да» - это единица, «нет» - это ноль.

Рассматриваемый подход применим как для ПП в целом, так и для отдельных модулей. Вопросы, предлагаемые разработчикам, делятся на три группы: в пользу применения для ПП (модуля ПП) автоматизации тестирования, за применение для ПП (модуля ПП) ручного тестирования, в пользу применения смешанного тестирования (автоматизация + ручное).

Опросные листы разработчиков поступают в отдел тестирования. Ведущий тестировщик, аналитик или руководитель отдела тестирования расставляет для каждого ответа долю важности.Доли выбираются из множества значений A = [0.25, 0.5, 0.75, 1]. Величина шага 0.25 выбрана опытным путем, как наиболее удобная для экспертной оценки.

В группе вопросов, говорящих в пользу автоматизации, единица означает, что с точки зрения данного критерия будет удобно пользоваться автоматизацией. Доля важности 0.75 означает, что автоматизация достаточно удобна, 0.5 – есть сомнения, что автоматизация будет удобна, 0.25 – есть сильные сомнения, что автоматизация будет удобна, 0 – автоматизация абсолютно не удобна. В группе вопросов, говорящих в пользу ручного тестирования, используется обратный принцип: ноль означает, что с точки зрения данного критерия будет удобно применять ручной подход к тестированию. Доля важности 0.25 означает, что ручной подход достаточно удобен, 0.5 – есть сомнения, что ручное тестирование будет удобно, 0.75 – есть сильные сомнения, что тестировать

вручную удобно, 1 – ручное тестирование абсолютно неудобно. В группе вопросов, посвященных смешанному тестированию, принцип ответов совпадает с группой вопросов автоматизации.

Поскольку оценка ноль при ее умножении на вес дает всегда ноль, предлагается ноль заменять на 0,25, а единицу на 0,75. Далее вычисляется свертка, диапазон значений которой лежит от -1 до 1 включительно. Положительное значение свертки говорит в пользу автоматизации тестирования, а отрицательное в пользу ручного тестирования. Данная свертка является объединением знаний разработчиков ПП и тестировщиков. Предложенный подход применим как для десктопных, так и для интернет-приложений. При определенной модификации вопросов, применим при тестировании мобильных приложений.

Горина Е.В., Иващенко Д.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РАСПРЕДЕЛЕННЫХ ПОЛИГРАФИЧЕСКИХ СИСТЕМАХ

Каждая типография или издательский комплекс представляет собой достаточно однородную структуру, которая стремится расширить спектр предоставляемых услуг. И при этом возникает необходимость сокращения расходов.

Выбор ИТ-решений для издательской деятельности весьма широк. Возможно привлечение специалистов для более профессионального выполнения изданий и пособий. Так, верстка может происходить как удаленно, так и на рабочем месте.

Преимущества удаленной работы известны всем:

- срочность исполнения работ;
- снижение накладных и операционных расходов;
- доступ к более широкому кругу исполнителей.

В полиграфических системах это становится возможным при условии, что большинство работников становятся удаленными:

- наборщик текста;
- корректор;
- верстальщик;
- макетировщик.

По сути на рабочем месте остаются только те, кому необходимо следить за самим техническим процессов изготовления изданий – рабочие, вальцовщики, которые прикрепляют и обложки. При этом система ИТ-решений включает в себя:

- CRM для учета рабочего времени и постановки задач;
- облако и общие файла для совместной работы;
- софт для общения с логированием переговоров;
- спецсофт для выполнения задач макетирования и иных задач.

При условии наличия денежных средств, сюда можно добавить:

автоматическую линию печати, что позволит обойтись без вальцовщика;

- службу доставки, что становится более выгодным для клиента;
- менеджера, так как привлечение клиентов можно сделать аутсорсингом, а документы предоставить почтой или курьером.

Результат – руководство можно осуществлять удаленно, а география подобной системы полиграфии составит весь мир. Сюда же можно включить – совместные удаленные офисы и печать по удаленной связи в регионах.

Горина Е.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОМОЩИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Сегодня каждый пользователь, имеющий доступ к интернету имеет возможность наблюдать за изменениями различных экономических показателей в реальном времени. Постепенно эти задачи стали переноситься и на мобильные платформы. Габариты мобильного устройства позволяют использовать его в любом месте, что имеет явное преимущество по сравнению с персональным компьютером. Развитие технологий 3G и 4G позволяет иметь доступ в интернет с телефона практически в любой точке, где только есть зона покрытия сотового оператора. Мобильные устройства поддерживают те же стандарты беспроводной радиосвязи Wi-Fi, что и персональные компьютеры.

Платформа Android удовлетворяет всем требованиям современной мобильной операционной системы, а так же ее повсеместное применение является положительным аспектом распространения

приложения. Разработка приложений для Android требует подготовить контент, осуществить подбор информационных материалов, разработать интерактивные составляющие приложения. Таким образом, приложение позволит максимально наглядно предоставить информацию для пользователя.

При создании мобильного приложения «Поддержки принятия решений при анализе инвестиций» под операционную систему Android, используется среда разработки Eclipse IDE и язык Java. Функциональная разработка оптимизирована под специфику современных мобильных устройств, на базе операционной системы Android. Основная функция приложения заключается в удобном представлении информации в виде графиков и новостной рубрики.

Востребованность данного проекта заключается в возможности совмещения материалов для графического и текстового анализа экономических показателей. Обороты рынка мобильных приложений и продажи смартфонов увеличиваются с года на год в разы, что способствует перспективе развития в направлении разработки мобильных приложений. Представленное приложение, совмещает в себе отображение графиков текущих котировок валют или акций и аналитических статей по ним, способствующих поддержке принятия решений.

Основным направлением совершенствования приложения является создание возможности обновления текущих изменений котировок акций и новостной ленты с занесением их в локальную базу на телефоне для работы в offline-режиме. Создание модели взаимодействия локальной базы в телефоне с глобальной (на сервере) посредством связи через интернет. Добавление специализированных методов статистического прогнозирования.

Приложение должно обеспечивать наглядность и доступность информации для пользователя. Пользовательский интерфейс является одним из важнейших конкурентных преимуществ любого программного продукта, поэтому организации и проведению работ по проектированию и дизайну должно уделяться максимальное внимание. Практически все приложения являются многоэкранными.

При запуске приложения пользователь попадает на главную страницу приложения. Стартовая страница состоит только из одного графического элемента – ImageView, которому соответствует фоновая картинка. Переход с начальной страницы на другие осуществляется через выбор соответствующего пункта меню. Приложение может показывать всплывающие сообщения с помощью класса Toast. Востребованность данного проекта заключается в возможности совмещения материалов для графического и текстового анализа экономических показателей. Обороты рынка мобильных приложений и продажи смартфонов увеличиваются с года на год в разы, что способствует перспективе развития в направлении разработки мобильных приложений. На данный момент на рынке приложений не представлено приложения, совмещающего в себе отображение графиков текущих котировок валют или акций и аналитических статей по ним, способствующих поддержке принятия решений.

Горлицкая С.И., Вострых А.И., Доценко А.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

СОЗДАНИЕ ИНТЕРАКТИВНЫХ ИНСТАЛЛЯЦИЙ НА ОСНОВЕ КНИЖНЫХ ИЛЛЮСТРАЦИЙ

Среди студенческих интерактивных инсталляций кафедры ИиУС ВШПМ СПГУПТПД весеннего семестра 2016 г появился целый ряд работ, в которых реализуются новые идеи. Во-первых, расширилась программная поддержка этих идей. Интерактивные инсталляции мы начали создавать на основе технологий web-дизайна и ядра JavaScript, а также с применением функций из подобранных студентом под конкретные задачи библиотек JavaScript.

Во-вторых, тематически значительно расширился круг художественных основ для интерактивных инсталляций. Одно из направлений – использование книжных иллюстраций, в частности - волшебный мир художника Низовцева.

Новые идеи этого года – подбор и настройка анимационных библиотек CSS, как уже готовых методов анимации, так и создаваемых в процессе анимирования. К примеру, из большого множества анимационных библиотек Вострых отобрала такие как: Animated.css, Awesome.css, Jquery.js, Magic.css и другие. При помощи разнообразных методов создания анимации в представленных библиотеках организуется движение, исчезновение, появление, трансформация объектов.

Создание интерактивных инсталляций, выполнение Алёной Доценко, также основывается на книжных иллюстрациях художника Низовцева. Из многочисленных произведений художника были отобраны картины «И настала звёздная ночь», «Звезды рядом», «Лебедь-сказка». Сказочный характер картин и переданное художником волшебство требовали особой точности при подборе библиотек. Доценко предложила анимационные библиотеки Animated.css, Hover.css, Jquery.js, Magic.css. И их помощью удалось реализовать интерактивную анимацию. При наведении курсора мышь на различные элементы приводится в действие соответствующая анимация, передавая тем самым ощущение присутствия. Всё это позволяет интерактивно погрузиться в волшебный мир книжной иллюстрации. Пожалуй, это можно интерпретировать как создание некого альтернативного

представления картины с дополнением ее различными объектами, как попытка расширения ощущаемых эмоций, передаваемых автором книжной иллюстрации.

Груздева И.Г., Дмитрук В.В., Шелохова Е.Н.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ВЛИЯНИЕ ТЕХНОЛОГИЙ «HD_FLEXO» И «DIGI FLOW» НА КАЧЕСТВО ПЕЧАТИ

Технологии допечатного производства довольно широко представлены на современном мировом рынке. Проведенный анализ технологий для флексографской печати показал, что цифровая технология «HD-Flexo» высоко частотного растрирования позволяет проводить запись печатных элементов на фотополимерных пластинах с частотой 4000 dpi, вместо традиционных 2540 dpi. Это обеспечивает меньшую ступенчатость при передаче тонов, а также дает возможность формировать микроячейки на поверхности плашки, позволяющие увеличивать краскоперенос. С применением технологии «Digi Flow» появляется возможность проводить экспонирование с так называемой контролируемой атмосферой, что снижает процесс ингибирования фотополимера кислородом воздуха, при этом цоколь печатного элемента формируется более плоским, что приводит к уменьшению растискивания при печати.

Для подтверждения теоретических данных проведены практические исследования. Специально изготовлены печатные формы на пластинах Cyrel® типа DPR (толщина 1,14 мм) с применением традиционных и исследуемых технологий и проведена тестовая печать на машине FP 16S (Fischer&Krecke, Германия) красками с вязкостью 18 – 22 секунд по невпитывающей поверхности.

Стабильность печати оценивали путем выборки по 5 экземпляров через каждые 100 тысяч оттисков и измерения оптической плотности на тест-объектах с помощью денситометра. Выявлено, что оптическая плотность и равномерность печати выше в среднем на 5 - 10 % при применении технологии высокочастотного растрирования и экспонирования с контролируемой атмосферой, несмотря на то, что краскоперенос - ниже на 4 % (определен путем взвешивания оттисков). Распределение краски внутри штриха равномерное. Более плоский цоколь печатного элемента обуславливает уменьшение давления в печатной паре, красочный слой не вытесняется от центра к краям, не формируется ярко выраженный ореол по контуру печатного элемента, что способствует повышению удобочитаемости текста.

Полученные результаты подтвердили целесообразность применения технологий «HD-Flexo» и «Digi Flow» для подготовки макетов и изготовления печатных форм, содержащих большое количество плашек и текста с мелким кеглем.

Груздева И.Г, Кудрин Ю.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

РАЗРАБОТКА СПЕЦИАЛЬНЫХ КРАСОЧНЫХ СОСТАВОВ НА ОСНОВЕ НЕОРГАНИЧЕСКИХ ЛЮМИНОФОРОВ ХАЛЬКОГЕНИДНОЙ ГРУППЫ ДЛЯ ЗАЩИТЫ УПАКОВОЧНОЙ ПРОДУКЦИИ ОТ ФАЛЬСИФИКАЦИИ

При изготовлении упаковки фармацевтической продукции высокой стоимости, товаров для инструментальных и авто-производств и прочих высокомаржинальных секторов промышленности используют различные способы полиграфической защиты от фальсификации (металлография (интаглио), ирисный раскат, дифракционные элементы и др.), но для рынка потребительских товаров эти технологии недоступны, т.к. затраты на них в данном случае неоправданно велики.

Одним из перспективных и относительно недорогих способов защиты является разработка специальных красочных составов (с применением отечественных неорганических люминофоров), приготовление которых возможно непосредственно на полиграфических предприятиях.

К экспериментальному красочному составу предъявляются следующие требования:

- простая идентификация, доступная потребителю;
- нанесение с помощью существующих способов печати;
- отсутствие необходимости модернизации печатных узлов;
- низкая себестоимость;
- максимальное содержание компонентов отечественного производства;
- стабильность в печатном процессе;
- технология изготовления, применимая в условиях типографии.

В Санкт-Петербурге в течение нескольких лет проводится работа по созданию модельных красочных составов на основе люминофоров халькогенидной группы производства ЗАО Люминофор (Ставрополь). Эти люминофоры доступны, хорошо изучены и сравнительно недороги.

Данное исследование посвящено композициям на основе сульфида цинка, активированного ионами меди (ZnS-Cu), для флексографских красок УФ-отверждения, поскольку флексография является одним из наиболее востребованных способов печати на упаковке. Такие люминофорные

составы излучают в УФ-А диапазоне (365 нм), а прибором для визуализации может служить обычный бытовой УФ-диодный фонарик.

Основные проблемы, возникающие при изготовлении подобных составов, связаны с осаждением частиц вследствие их высокой плотности (более 4 г/см^3), забиванием ячеек анилоксового вала и ухудшением краскопереноса и, как следствие, с уменьшением степени свечения. Главным параметром, влияющим на протекание всех этих процессов, является гранулометрическая характеристика люминофорной композиции.

Исходя из этого, в работе поставлены и решены следующие задачи:

- подбор степени дисперсности частиц, которая позволяет сохранить приемлемый уровень яркости свечения и устойчивость красочного состава к расслаиванию;
- определение массовой доли (концентрации) люминофора, обеспечивающей необходимые реологические характеристики краски;
- отработка технологии получения модельных составов в условиях типографии;
- печать тестовых тиражей и контроль качества оттисков по уровню свечения.

Выбранный гранулометрический ряд (10,2 мкм, 4,5 мкм, 2,0 мкм и 1,2 мкм) позволил оценить весь доступный диапазон возможных размеров, т.к. частицы диаметром более 10,5 мкм не позволяют сохранить стабильность печати (наблюдается расслаивание композиции), а диаметром менее 0,5 мкм - практически не работают (низкий квантовый выход). После анализа степени свечения полученных тестовых оттисков с помощью комплекса PIA-8 (Projectina AG, Швейцария) для дальнейших экспериментов остановились на фракции с размером частиц 4,5 мкм.

Весовая концентрация люминофора на первой итерации составляла 15% (т.е. средняя теоретическая концентрация пигмента в краске для флексографской печати). Также рассматривались концентрации 10, 12 и 18%, соответственно. Оттиски, отпечатанные при тех же условиях, что и предыдущий тестовый тираж, при облучении 40-ваттной УФ-А лампой, показали, что степень свечения у составов с концентрацией люминофора 12% и 15% практически одинаковая, а у состава с концентрацией 18% немного выше. Но при детальном рассмотрении печатной системы было замечено, что в случае 18% - концентрации частицы люминофора остаются как на поверхности дуктора, так и на стенках и ячейках анилоксового вала, что говорит об избыточном их количестве. Учитывая стоимость люминофоров, для изготовления рабочих тиражей приняли концентрацию 12%.

Чтобы обеспечить повторяемость свойств получаемых в дальнейшем красочных композиций, разработали трехступенчатый процесс замешивания с помощью лабораторного диссольвера Лаботекс ЛДУ 3-МПР (Россия). Технология позволяет получать составы без разрушения частиц люминофора вследствие значительных механических воздействий. В качестве основных параметров на каждом этапе фигурируют: время, скорость, температура смешения, тип мешалки. Во избежание образования крупных агломератов (более 50 мкм) предусмотрена добавка 5% диспергатора Disper BYK 108. В качестве прозрачной основы для красочной композиции использован продукт Transparent White от Flint Group.

Пилотные тиражи, отпечатанные по разработанной технологии, получили высокую оценку заказчиков. В процессе работы замечаний по качеству печати, стабильности свечения и поведения краски не было. В дальнейшем планируется изготовление защитных составов, оптимизированных под другие полиграфические технологии.

Авторы выражают признательность коллегам из НИИ ГоЗнак (Санкт-Петербург) и НИИ ИРЭА (Москва) за помощь и техническую поддержку.

Гнатюк С.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна, Санкт-Петербургский государственный институт кино и телевидения

ОЦЕНКА ВЛИЯНИЯ ГЕОМЕТРИЧЕСКИХ И СОРБЦИОННО – АДГЕЗИОННЫХ СВОЙСТВ ЗАПЕЧАТЫВАЕМЫХ МАТЕРИАЛОВ НА КАЧЕСТВО РЕПРОДУКЦИИ НА ОСНОВЕ РЕЗУЛЬТАТОВ МАТЕМАТИЧЕСКОГО ОПИСАНИЯ СВЯЗИ ИНТЕГРАЛЬНОЙ ОПТИЧЕСКОЙ ПЛОТНОСТИ ИЗОБРАЖЕНИЯ ТЕСТ - ОБЪЕКТА И РАЗРЕШАЮЩЕЙ СПОСОБНОСТИ В СИСТЕМАХ ЦИФРОВОЙ СТРУЙНОЙ И ЭЛЕКТРОФОТОГРАФИЧЕСКОЙ (ЭЛЕКТРОГРАФИЧЕСКОЙ) ПЕЧАТИ

Системный подход к оценке результатов репродукционного процесса с использованием репрезентативной выборки материалов для цифровой струйной и электрофотографической (электрографической) печати привел к определению перечня параметров печатной копии оригинала тест - объекта, крайне чувствительных к вариативности особенностей структуры подложки, которая может быть описана предлагаемым автором уникальным комплексом ее геометрических и сорбционно - адгезионных характеристик, часто находящихся в синкретическом взаимодействии.

Так, при описании особенностей микрогеометрии использованы методы, основанные на представлениях о ее мультифрактальной природе, что позволило судить о выраженности структурных особенностей материала, равномерности в распределении микронеоднородностей на единице площади или объема, связанности образуемых ими кластеров и т.д. (такой подход наиболее

обоснован при исследовании топологии материалов со стохастическим распределением поверхностных свойств).

Оценка сорбционно – адгезионных характеристик проводилась посредством анализа результатов взаимодействия окрашенных и неокрашенных компонент красок с поверхностью и объемом запечатываемого материала на основании изучения особенностей микроизображения специально сформированного тест – объекта.

Использование методов корреляционного и регрессионного анализа показало амбивалентный характер связей, позволило осуществить их ранжирование на основании количественной оценки степени их релевантности, а также учесть их зависимость от метода формирования изображения.

При постановке целей и задач исследования был сделан акцент на поиск прикладных методов измерений, не требующих привлечения эксклюзивного оборудования с одной стороны, и позволяющих оперативно получать и интерпретировать результаты измерений с другой стороны. Показано, что эти условия выполнимы путем количественной оценки величины интегральной оптической плотности изображения полей специально сформированного тест – объекта - штриховой миры с одинаковой шириной запечатанных и пробельных элементов.

Как оказалось, форма регрессии интегральной оптической плотности от варьируемой в широких пределах частоты следования штрихов крайне чувствительна и к выбранной технологии формирования изображения, и к качеству используемого материала, а ее на первый взгляд эмпирические коэффициенты обладают высокой степенью воспроизводимости и однородности и могут быть использованы в качестве информационных маркеров, своеобразных интегральных критериев оценки текущего состояния репродукционного процесса (например, стабильности) или на этапе входного контроля качества полиграфических (расходных) материалов.

На взгляд автора, предложенный подход и результаты исследования могут оказаться принципиально важными и в тех случаях, когда к печатной копии предъявляются повышенные требования в отображении, например, мелких деталей изображения, что характерно для технологий производства широкого спектра промышленных изделий, в основу которых положены либо принципы традиционной полиграфической печати, либо методы цифровой печати (в том числе 3D печать).

В предыдущих исследованиях было показано, что роль комплекса сорбционно – адгезионных свойств запечатываемого материала можно довольно легко количественно оценивать, например, на основании формы гистограммы изображения тест – объекта, аналогичного используемому в настоящей работе, либо его характерных элементов (дисперсии границы запечатанного элемента растра) и т.д. Их дальнейшее развитие позволило усовершенствовать эти методики и математически описать (а в результате контролировать, прогнозировать) влияние этой группы свойств на величину возникающих в результате искажений.

Ввиду относительной простоты предложенный подход можно использовать в режиме «реального времени» для непрерывного мониторинга текущего состояния печатного процесса, адаптировать его для включения в технологические линии производства печатных материалов, и использовать его при создании систем технического зрения, используемых для контроля состояния группы родственных процессов.

Кайнарова Е.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна

ГЕНЕРАТИВНЫЙ ДИЗАЙН КАК ИНСТРУМЕНТ ДЕЯТЕЛЬНОСТИ ДИЗАЙНЕРА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И МЕДИА ИНДУСТРИИ

Тенденции развития современных медиатехнологий показывают, что программирование становится новым, дополнительным инструментом деятельности дизайнера для создания творческих проектов. Развитие информационных технологий, новых инструментов и технологий в сфере дизайна открывают возможности для воплощения любых идей. Формализация процессов создания интерактивных инсталляций, визуализации данных, анимации, проектирования архитектурных объектов заложена в концепцию генеративного дизайна. Генеративный дизайн - это метод проектирования, в котором итоговый продукт - изображение, звук, архитектурные модели, анимация - создается с помощью набора правил и алгоритмов. В результате программирование становится неотъемлемой частью создания любого медиа-проекта, что способствует появлению понятия креативного программирования. Идеи генеративного дизайна основываются на параметрическом моделировании. Это один из быстрых методов исследования дизайнерских возможностей.

В условиях конкурентного сосуществования на рынке организаций, предлагающих дизайнерские услуги, немаловажными факторами становятся временные затраты на разработку дизайна продукта, а также количество предоставляемых заказчику вариантов дизайна. Таким образом, необходимо обеспечить дизайнера методом, позволяющим в автоматизированном режиме создавать необходимое количество вариантов дизайна продукта с последующей интеграцией их в технологический процесс.

Канатенко М.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ЦИФРОВОЙ ПЕЧАТИ

В последние 10 -15 лет, в связи с развитием средств массовой информации, все большее значение имела новизна и скорость получения информации. Если говорить о направлении информационного потока, связанного с печатными средствами информации, то все отчетливее проявлялась тенденция к снижению тиражей, повышению их целевой направленности, увеличению скорости доставки потребителю. Этим требованиям традиционные виды печати, такие как плоская офсетная, высокая или глубокая уже не отвечали, вследствие присутствия постоянных печатных форм, трудоемкости формных процессов и приладочных работ, нерентабельности печати малых тиражей. В результате, на смену данным классическим видам все чаще приходили цифровые печатные технологии, которые были наиболее адаптированы под современные требования информационного рынка. Этому способствовало бурное развитие в 90-х годах компьютерной техники и повсеместное внедрение этой технологии в печатное дело.

В настоящее время цифровые печатные технологии уже не ограничиваются полиграфией. Стремительно расширяется сектор применения этих технологий и в других отраслях. Так, например, появилась печатная электроника – печать электронных схем и компонентов токопроводящими или светящимися красками, изготовление экранов и дисплеев. Интересны и перспективны технологии изготовления интерактивной SMART упаковки, создание анимированных иллюстраций. Несомненно, лидирующие позиции сегодня занимает 3D печать – изготовление печатным способом объемных предметов и моделей. В результате цифровая печать начинает активно внедряться в различные современные технологии.

Капуста Т.В., Яковлев П.О.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ИССЛЕДОВАНИЕ ПЕЧАТНО-ТЕХНИЧЕСКИЕХ СВОЙСТВ РАСХОДНЫХ МАТЕРИАЛОВ ОФСЕТНОЙ ПЕЧАТИ

Технология офсетной печати на листовых машинах предъявляет определенные требования к свойствам применяемых расходных материалов. Причиной многих дефектов печатной продукции может быть несоответствие печатно-технических свойств используемых материалов условиям проведения печатного процесса, или представленные в паспортных данных показатели свойств материалов не дают полной возможности оценить их поведение в процессе печати, или же их измеренные рабочие характеристики не всегда соответствуют требованиям, предъявляемым к ним. В связи с этим, в одной из типографий Санкт-Петербурга возникла необходимость в подборе расходных материалов для листовой офсетной печати на однокрасочной машине «Ryobi 520».

Объектом исследования стали печатно-технические свойства ассортимента бумаг, красок, офсетных резинотканевых полотен (ОРТП) и составы увлажняющих растворов (УР), обеспечивающие нормируемые качественные показатели. Цель работы была обозначена как – выявление соответствия измеренных параметров исследуемых материалов паспортным данным или рекомендованным нормам и оценка целесообразности использования этих материалов в рассматриваемом технологическом процессе.

Для печатания офсетным способом используется большой ассортимент бумаг, которые классифицируются по многим признакам, но основными требованиями, предъявляемыми к ним, являются: высокая прочность поверхности к выщипыванию и минимальная деформация при увлажнении. При исследовании печатно-технических свойств бумаг Maestro Print Syktyvkar; Mega Coat Gloss HB C2S; Galeri Art Gloss; Crystal Board (C1S) были определены следующие их параметры: масса 1м^2, толщина, плотность, средний размер пор, впитывающая способность, скручиваемость при одностороннем смачивании, линейная деформация при увлажнении, гладкость и стойкость поверхности к выщипыванию. Анализ полученных результатов выявил, что основные технологические характеристики рассматриваемых бумаг соответствуют норме, а повышенная неоднородность структуры некоторых из них и высокий показатель скручиваемости может привести к снижению качества оттисков и проблемам в процессе их дальнейшей обработки.

Печатно-технические свойства красок влияют на их поведение в печатном процессе: способность раскатываться и накатываться на поверхность печатной формы, переходить под давлением на запечатываемый материал и закрепляться на нем, создавая качественное изображение. Для серии триадных красок «Process Mateplus» были определены такие параметры, как степень их растекания и перетира. Анализ полученных экспериментальных данных выявил, что степень перетира для всех красок триады и степень растекания по черной краске – соответствуют нормам. Степень растекания по г,п,ж краскам – превышает нормируемые значения, что стоит учесть при регулировании баланса краска-вода.

Большую роль в офсетной печати играет многокомпонентный УР, а его правильный выбор по составу и рабочим параметрам влияет на стабильность и качество печатного процесса. Задача исследования состояла в изучении изменения параметров УР от состава его компонентов (различных буферных добавок - «Hydrospeed AFS 311» и «K Gold Fount», наличия/отсутствия ИПС), а также в выявлении их влияния на рабочие свойства самого увлажняющего раствора и печатно-технические характеристики краски. Поэтому в ходе исследования были определены: параметры используемой в типографии водопроводной воды; составы УР, обеспечивающие их стандартные параметры; величины краевых углов смачивания различных по составу УР на поверхности ОПФ; степень эмульгирования пурпурной краски (эмульсии: В/М, М/В) с различными по составу УР. Анализ экспериментальных данных позволил подобрать оптимальный состав УР с нормируемыми параметрами (pH=4,8; электропроводность 1124 мкСм при $dH_{воды}$=5°), т.е. с использованием 3% добавки «Hydrospeed AFS 311» без добавления ИПС.

Декельная композиция, в состав которой входит ОРТП, играет в офсетной печати важную роль: помимо создания равномерного давления в полосе печатного контакта, она осуществляет краскоперенос. Поэтому очень важен правильный выбор печатно-технических и деформационных свойств ОРТП в соответствии с технологическими задачами печатания. В ходе исследования печатно-технических свойств ОРТП («Sun DOT» и «Privilege») были определены их следующие параметры: толщина; шероховатость краскопередающего слоя, его твердость и стойкость к набуханию в различных жидкостях, а также величина краевого угла смачивания его поверхности водой и деформационные свойства. Анализ результатов исследования показал, что оба полотна – мягкие, имеют нормируемые значения абсолютной и относительной деформаций сжатия; рабочая поверхность полотна «Privilege» – более устойчива к смывкам, а «Sun DOT» – к связующим красок; ОРТП «Privilege» имеет более шероховатую рабочую поверхность, поэтому его можно рекомендовать для печати на бумагах без покрытия и картонах, а более гладкое полотно «Sun DOT» - для печати на мелованных бумагах.

Результатом проделанной работы стали технологические рекомендации к выбору расходных материалов и работе с ними, с учётом особенностей печатного процесса на однокрасочной листовой офсетной машине «Ryobi 520», что позволило уменьшить количество выпускаемого брака, снизить непроизводительные простои печатного оборудования и повысить качество издательской продукции.

Капуста Т.В., Абросимова Н.И., Абраменкова Ю.С.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ТЕХНОЛОГИИ ПЕЧАТИ ПО ТКАНЯМ

Развитие оперативной полиграфии позволило расширить ассортимент запечатываемых материалов, добавив к ним текстиль, что в свою очередь вывело печать по тканям на новый уровень. В настоящее время этот сегмент рынка пользуется огромным спросом у заказчиков.

Для запечатывания синтетических тканевых материалов в одной из типографий Санкт-Петербурга успешно применяют технологию сублимационной печати. Также, для повышения конкурентоспособности, привлечения новых заказчиков и увеличения количества наименований выпускаемых тканевых изделий в производство был взят аналог (по структуре) синтетической ткани - натуральная хлопковая ткань, для запечатывания которой осваивается метод каплеструйной печати.

Таким образом, для печатания по различным тканевым материалам в типографии стали применять две разные технологии – сублимационную и цифровую. Соответственно, используемые в них расходные материалы отличаются по своим свойствам и репродукционные возможности способов, имеющих свои характерные особенности, влияющие на качество оттисков, также различны. В связи с этим, возникла необходимость в подборе и отработке технологических режимов печатных процессов для различных по характеру изображений на ассортименте запечатываемых тканевых материалов и оценке качества полученных оттисков.

Задачей данной работы являлось выявление характера влияния технологических особенностей печатного процесса как на качество оттисков, так и на эксплуатационные свойства готовых изделий.

Анализ литературных источников показал, что метод сублимационной печати включает в себя два технологических этапа: нанесение зеркального изображения на промежуточный носитель (сублимационную бумагу) и перенос с него изображения на ткань посредством диффузии при ее нагревании. При переносе чернила почти целиком покидают поверхность сублимационной бумаги, которая их не удерживает. После прохождения через печатающие пьезоголовки принтера чернила в виде микрокапель впитываются в пористое покрытие бумаги, а частицы красителя оседают на поверхности. Формируемое ими зеркальное изображение выглядит достаточно бледным, но после термосублимации и диффузии в полимер изображение становится ярким и насыщенным. В технологии сублимационной печати следует использовать полиэстеровые и смесовые ткани, но обязательно с 70 %-м содержанием полиэфирного волокна.

Технология каплеструйной печати предполагает прямую печать на ткани без промежуточных носителей изображения. Для различных по составу тканей используются соответствующие активные или кислотные красители, а для печати по хлопку - водные пигментные чернила. Вне зависимости от состава ткани, она подвергается предварительной обработке праймером – водной дисперсией, предотвращающей слишком активное впитывание текстильных чернил в материал, и обеспечивающей хорошую адгезию красителя.

Для сравнения репродукционных возможностей рассматриваемых технологий была проведена печать тестового изображения на тканевых материалах Кулирка (сублимационная печать) и Кулирка 100% хлопок (каплеструйная печать). Сублимационная печать осуществлялась на плоттере «Mimaki JV4-160» с последующим термопереносом на каландровом термопрессе «CORONA 1700», а для каплеструйной печати использовался текстильный принтер «Epson SureColor».

При оценке качества полученных тестовых оттисков на рассматриваемых тканевых материалах измерялись, рассчитывались и оценивались следующее единичные показатели качества оттисков: ширина минимально воспроизводимого штриха в негативе и позитиве, размер кегля шрифта в негативе и позитиве, минимальная и максимальная оптическая плотность, эффективный градационный интервал, контраст печати, равномерность красочного слоя.

Было установлено, что в прямой каплеструйной печати обеспечиваются более высокие выделяющая способность и равномерность красочного слоя на оттиске, а в сублимационной - - наибольший эффективный градационный интервал, интервал печати и относительный контраст оттиска.

Также были оценены показатели качества оттисков после их термомеханической обработки, которой подвергаются готовые изделия в процессе эксплуатации (стирка со стиральным порошком, влажное глажение). Эти воздействия не оказывают влияния на выделяющую способность изображений на оттисках, но увеличивают их оптическую плотность; степень наравномерности распределения красочного слоя - уменьшилась. Выявленные изменения на оттисках характерны для обеих технологий.

По результатам исследования можно рекомендовать сублимационную технологию для воспроизведения крупных штриховых элементов изображения, а каплеструйную - для детализированных штриховых и тоновых изображений.

Результаты работы представлены в виде технологических рекомендаций по печати на ассортименте тканевых материалов в конкретных производственных условиях.

Коваленко А.Н.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ: ФОРМЫ И СВОЙСТВА

В литературе увеличивается использование термина «виртуальная реальность». Это требует изучения относительно нового понятия и исследования его связи с реальностью. Обычно виртуал жестко противопоставляется реалу, но мы попробуем показать, что это не вполне так. Возникновение термина «виртуальная реальность» обычно привязывают к появлению поколения компьютерных игр, где объекты игр, фон (среда), движение и звук выполняются на высоком уровне соответствия реальности (используются специальные очки, наушники, движение кресла и др.). Но само понятие, безусловно, выходит за пределы игр и связано с ощущениями и мировосприятием человека вообще.

Мы исходим из объективности существования реального мира и предлагаем рассуждать о виртуальных мирах как о вариантах или моделях реальности. Удобно использовать термин «сдвинутая реальность», которому можно приписывать разную степень отличия от реала.

Значительные элементы ухода от реальности присутствуют в некомпьютерных играх, например, в казино, а также при интернет-зависимости. Человек не вполне ощущает себя в реале в таких состояниях как стресс, тяжёлые переживания и тяжёлая болезнь, влюблённость, погружение в фантазии, эйфория. Реальность ещё более сдвинута в таких состояниях как психические расстройства, воздействие психотропных веществ, гипноз. Отдельную группу «сдвинутой реальности» образует погружение в мир книги, спектакля, кинофильма. И, наконец, вершиной виртуальной реальности является сон.

Сну приписываются такие отличия от реальности как спонтанность, фрагментарность, только частичная причинность и сложная связь с реально имевшими место событиями. Во сне в изменённом виде выступают личность, сознание, телесность.

Существующая компьютерная виртуальность уводит человека от реальности пока на уровне кино и театра, и, в принципе, позволяет ему в любой момент выйти в реал. Развивающиеся медиатехнологии стремятся «затянуть» человека в этот мир все сильнее, в этом надо видеть потенциальную опасность. Футурологи уже говорят о том, что в будущем человек сможет жить в нескольких мирах, только один из которых будет реальным.

Всё это говорит о необходимости исследования компьютерной виртуальной реальности и тенденций её развития.

Костюк И.В., Козлова И.А., Алферов Н.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ЭФФЕКТИВНОГО ИСПОЛЬЗОВАНИЯ ИНТЕНСИВНЫХ КРАСОК В ОФСЕТНОЙ ИЛЛЮСТРАЦИОННОЙ ПЕЧАТИ

Некоторые категории полиграфической продукции (например, художественные издания, содержащие изображения авторских работ) требуют высокой точности воспроизведения иллюстрационной компоненты, что, по крайней мере, предполагает визуальное тождество печатной репродукции и оригинала. Данная задача определяет одно из направлений усовершенствования полиграфического процесса: устранение ограничений его репродукционных возможностей, в частности, в отношении цветовоспроизведения.

На сегодняшний день разработано множество технологических решений, направленных на расширение цветового охвата печати и интервала воспроизводимых градаций (Hi-Fi технологии, печать смесевыми и интенсивными красками и др.). Использование интенсивных красок - достаточно простая в технологическом отношении альтернатива традиционной ГПЖЧ печати. Интенсивные краски обеспечивают более высокие оптические плотности на оттиске при меньшей толщине красочного слоя, что обусловлено меньшим размером частиц пигмента, более высокой его концентрацией и лучшей диспергируемостью пигмента в связующем. Широкому применению интенсивных красок, в частности, в офсетной иллюстрационной печати препятствуют противоречивые оценки их технологических и репродукционных возможностей. Анализ источников технической информации продемонстрировал недостаточность объективных данных, подтверждающих или опровергающих данные оценки. В связи с этим представляется актуальным исследование эффективности применения интенсивных красок для расширения цветового охвата офсетной печати, анализ целесообразности их использования и определение области возможного применения.

Сообразно этой задаче в данной работе проведен ряд исследований, основанных на применении методов инструментального анализа, которые имеют объективный характер. Так, выполнена спектрофотометрическая и денситометрическая оценка спектральной чистоты основных цветов офсетных красок обычной и интенсивной триады, а также колориметрическая оценка светлоты и насыщенности комбинированных цветов (в метрике равноконтрастной системы LCH МКО), воспроизводимых обычной и интенсивной триадными красками.

Анализ спектральных характеристик основных цветов двух триад показал, что голубой и пурпурный цвета интенсивной триады характеризуются бóльшим поглощением в основной зоне спектра, но и бóльшим уровнем вредного поглощения в дополнительных областях (особенно пурпурная). Таким образом, спектрофотометрический анализ не позволил сделать выводы о преимуществе интенсивных красок перед традиционными в спектральном отношении. Для более объективной оценки также проводился денситометрический анализ двух триад, более грубый (трехзональный), но предоставляющий возможность получения количественных показателей спектральной чистоты основных цветов (ахроматичности, сдвига (ошибки) цветового тона и эффективности цвета). Однако для пурпурной интенсивной краски были отмечены: более высокий показатель ошибки цветового тона (41% против 37% у обычной краски) и более низкий показатель эффективности цвета (82% против 84%). Для голубой интенсивной краски зафиксирован более высокий показатель ахроматичности цвета (18% против 15% у обычной краски). Таким образом, и денситометрическая оценка спектральной чистоты цветов не позволила судить о преимуществах интенсивных красок перед традиционными и об эффективности их применения для расширения возможностей триадной печати в отношении цветопередачи.

Несмотря на полученные выводы, различие спектральных характеристик основных цветов сравниваемых триад может оказать влияние на колориметрические показатели воспроизводимых ими цветов, т.е. на их восприятие, испытываемое наблюдателем в заданных условиях внешнего освещения. Колориметрическая оценка позволила констатировать некоторые преимущества применения интенсивных красок в отношении тоно- и цветовоспроизведения и сформулировать рекомендации по допечатной подготовке изобразительной информации.

Так, были отмечены более низкие значения светлоты воспроизводимых интенсивными красками цветов (особенно, в диапазоне от средних до темных тонов), что требует создания специального цветового профиля для проведения цветоделения изображений и моделирования результатов печати на допечатной стадии.

Различие в изменении светлоты воспроизводимых интенсивными красками светлых и темных цветов позволяет судить о большем локальном и детальном контрасте печатной репродукции. Это преимущество данных красок будет востребовано для изображений, требующих точности передачи контурной составляющей.

Обеспечиваемое интенсивными красками повышение насыщенности светлых цветов может быть востребовано для воспроизведения изображений, содержащих пастельные оттенки.

Костюк И.В., Малеваный К.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ ВОСПРОИЗВЕДЕНИЯ ИЗОБРАЖЕНИЙ СПОСОБОМ КАПЛЕСТРУЙНОЙ ПЕЧАТИ

Одной из наиболее перспективных и развивающихся технологий цифровой печати является каплеструйная печать. Анализ технической информации о современных каплеструйных печатных устройствах позволил установить основные направления их совершенствования:

- увеличение репродукционного потенциала систем многокрасочной печати;
- повышение устойчивости печатных репродукций к внешним воздействиям;
- разработка и совершенствование систем тиражной печати (основные усилия направлены на снижение себестоимости оттисков и увеличение производительности оборудования);
- расширение функционала печатающих устройств, например, за счет объединения в одном устройстве преимуществ печати цветных тоновых оригиналов водорастворимыми чернилами и черно-белой печати штриховых оригиналов чернилами на основе пигментов.

Активная работа ведущих компаний-производителей каплеструйного печатного оборудования (Epson, Canon, HP, Lenmark и др.) в этих направлениях позволяет предположить актуальность проведения исследования возможностей этой технологии печати в отношении обеспечения точного (визуально-тождественного) воспроизведения изображения.

Одной из серьезных проблем, препятствующих полноценному использованию потенциала каплеструйной печати, является применение печатных систем «устройство-драйвер». Отсутствие растрового процессора, являющегося единым обрабатывающим звеном, открытым для управления, обуславливает и другие проблемы технологического характера:

- неоднозначность трактовки цвета в условиях многовариантности программных средств допечатной подготовки оригинал-макетов;
- отсутствие возможности управления параметрами воспроизведения оригинал-макетов различного информационного содержания;
- отсутствие регламента управления цветом и, как следствие, сложности в обеспечении достоверного и предсказуемого результата при печати.

Основной задачей данной работы было выявление способов увеличения и эффективного использования репродукционного потенциала каплеструйных печатных систем конфигурации «устройство-драйвер». В качестве объекта исследования использовалось пьезоэлектрическое печатное устройство Epson Stylus Photo PX660. Основные исследования были сосредоточены на оценке эффективности различных подходов к управлению цветом в компьютерной издательской системе в обеспечении точности тоно- и цветовоспроизведения. В качестве основных критериев оценки по результату печати были выбраны: точность цветопередачи, линейность градационных характеристик и обеспечение общего цветового баланса в воспроизводимом градационном диапазоне. Для проведения исследований был разработан тест-объект, содержащий ступенчатые шкалы единичных и бинарных цветов, равноконтрастную трехкрасочную шкалу, нестационарные элементы памятных цветов, градиентные растяжки и др. Все исследования проводились с использованием методов инструментальной (колориметрической) оценки.

Для обеспечения достоверности цветопередачи необходимо разработать стратегию управления цветом. На первом этапе должны быть определены режимы печати (например, уровень подачи чернил, разрешение печати и т.д.) для каждого запечатываемого материала. Главным критерием выбора является обеспечение максимального эффективного интервала плотностей тоновой репродукции. Основным инструментом управления цветом является цветовой профиль, который создается индивидуально для каждого устройства и системы, задействованных в репродукционном процессе. Для построения цветового профиля каплеструйной печати, важно выбрать шкалу цветового охвата и графический редактор, позволяющий отключить управление цветом при ее воспроизведении, т.к. от этого зависит объективность оценки характеристик передачи цвета печатной системы. Также при построении цветового профиля необходимо сделать обоснованный выбор алгоритма интерполяции и метода преобразования цветовых значений.

Цветовой профиль печати может быть использован в компьютерной издательской системе двумя способами, один из них предполагает управление цветом самой программой, выбранной для обработки изображений, а второй – подключение профиля в драйвер печатной системы. В исследуемой системе воспроизведения изображений для допечатной подготовки используется только программа Adobe Photoshop, которая позволяет при подключении цветового профиля для печати изображений выбирать метод преобразования цветов. Проведенные в работе исследования позволили выбрать способ использования профиля, который обеспечил визуально-тождественное воспроизведение цветных изображений.

Костюк И.В., Кюря В.П.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ТЕХНОЛОГИЯ УПРАВЛЕНИЯ ЦВЕТОМ ГЛУБОКОЙ ПЕЧАТИ НА ПОЛИМЕРНЫХ МАТЕРИАЛАХ С НЕСТАНДАРТНЫМИ ОПТИЧЕСКИМИ СВОЙСТВАМИ

Глубокая печать используется для изготовления продукции большими тиражами, в основном, этикеточно-упаковочной, для которой наиболее характерно: использование широкого ассортимента запечатываемых материалов; использование брендовых цветов, обуславливающее высокие требования к качеству цветопередачи; повторяющиеся тиражи, требующие стабильности результата печати.

Система управления цветом призвана обеспечить согласование всех стадий репродукционного процесса, однозначность трактовки цвета на всех технологических этапах, предсказуемость и достоверность воспроизведения информационного содержания оригинал-макета в тираже. В современных условиях реализации этикеточно-упаковочного производства, основанного на технологии глубокой печати, репродукционный процесс является открытым (разомкнутым). В связи с этим одним из наиболее важных процессов допечатной стадии становится моделирование результатов тиражной печати с использованием технологии цифровой цветопробы.

Основное требование к любой цветопробе – колориметрическое (визуальное) тождество будущей печатной репродукции.

В процессе подготовки оригинал-макета этикетки (упаковки) к воспроизведению способом глубокой печати, особенно при использовании нескольких смесевых цветов и нестандартных запечатываемых материалов, выполнение этого требования вызывает затруднения.

Так при моделировании цветов упаковки, воспроизводимой на материалах с нестандартными оптическими свойствами, в частности, на многослойном полимерном материале (ориентированный полипропилен, «жемчужное» покрытие, припрессованная матовая пленка) нередко возникают проблемы, связанные с соответствием цветов на цветопробе тиражному образцу. Последствия существования данной проблемы в той или иной степени проявляются в усложнении технологического процесса допечатной подготовки оригинал-макета этикетки/упаковки, которому сопутствуют дополнительные экономические и трудозатраты, а также возникает угроза потери постоянного Заказчика, наличие которого во многом определяет экономическую стабильность предприятия.

Для предотвращения этих негативных последствий необходима реорганизация системы моделирования результатов тиражной печати и системы управления цветом репродукционного процесса в целом. В связи с этим была определена цель данной работы – разработка технологических рекомендаций по созданию цветовых профилей цифровой цветопробной и тиражной печатных систем, задействованных в производстве этикетки на многослойном полимерном материале способом глубокой печати. Для достижения поставленной цели проведен ряд исследований в соответствии с разработанной методикой:

- оценка характера и степени отличия результатов цифровой и тиражной печати на многослойном полимерном материале и выявление возможных причин несоответствия;
- анализ условий печати при получении тестового оттиска;
- анализ влияния условий измерений цветов, воспроизводимых на многослойном полимерном материале, с использованием прибора со стандартной геометрией измерений;
- исследование влияния процедуры управления цветом цифровой цветопробы, в частности, условий создания цветового профиля печати, на объективность результатов моделирования печатной репродукции.

В результате проведенных теоретических и экспериментальных исследований были установлены возможные причины несоответствия цветопробы тиражному образцу:

- нарушение режимов тестовой печати (Fingerprint);
- некорректные условия оценки отпечатанной на материале с нестандартными оптическими свойствами шкалы цветового охвата, обуславливающее несоответствие визуальной и количественной оценки цветов на печатном образце;
- программные ошибки при построении цветового профиля печати и отсутствие количественных критериев выбора корректирующих воздействий при модификации автоматически сгенерированного цветового профиля.

Для решения данной проблемы сформулированы технологические рекомендации по процедуре управления цветом при подготовке оригинал-макетов этикетки/упаковки к воспроизведению способом глубокой печати:

- перед созданием цветового профиля печатной системы необходимо проведение оценки параметров печатного процесса (Fingerprint), в частности, характеристик приращения уровня тона;
- обязательна коррекция характеристик растискивания при модификации цветового профиля с учетом фактических значений, полученных при тестовой печати.

Макарова Н.Е
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ОСОБЕННОСТИ РЕАЛИЗАЦИИ БАЗОВЫХ ФУНКЦИЙ ОБРАБОТКИ ТЕКСТА В СОВРЕМЕННЫХ ИЗДАТЕЛЬСКИХ СИСТЕМАХ И ЗАДАЧИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЕРСТКИ

Задачи повышения эффективности и качества верстки являются достаточно актуальными как на этапе появления первых издательских систем, так и на современном этапе. Значительным образом на это влияет реализация базовых автоматизированных функций обработки текста.

Объектом исследования являются базовые функции обработки текста в Adobe InDesign и QuarkXpress, влияющие на эффективность и качество верстки.

Для анализа и сравнения работы функций в различных издательских системах проведено практическое исследование.

Для исследования использовались фрагменты изданий, содержащие тексты нескольких видов. После применения функций анализировались такие критерии, как удобочитаемость текста, единообразие верстки, соответствие сверстанных полос технологическим требованиям и отраслевым стандартам. Результаты работы функций для различных видов текстов сводились в таблицы и подвергались статистической обработке.

В результате проведенного исследования выявлены недостатки и упрощенный алгоритм реализации ряда функций: функции контроля линейности строк, высоты полос, пропорциональности интервалов между абзацами.

Предположительно, причиной упрощенного построения алгоритмов является интеграция в современных издательских системах функций классической обработки текста с функциями создания мультимедийных изданий, что привело к ослаблению внимания разработчиков к базовым операциям.

По результатам анализа проведенного исследования, сравнения функций в издательских системах предыдущего поколения, классических технологий верстки предлагается методика повышения эффективности обработки текста и способы ее реализации.

Лысенко В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна

ТЕОРИЯ СОЗДАНИЯ. РАЗВИТИЕ

Ранее рассмотрены ключевые положения теории создания объектов живой и неживой природы [Лысенко В.А. Теория создания //Материалы международной конференции "Региональная информатика - 2014", СПб, СПОИСУ. – 2014, с. 505-506]. Показано, что процесс создания носит универсальный характер и развивается по установленному алгоритму.

Проведенный анализ позволяет адекватно описывать жизненный цикл создаваемого объекта как путь проекции движения во времени информации (идеи) при ее материальном воплощении и управлять этим процессом, воздействуя на потоки ресурсов (материальных, интеллектуальных, людских, технологических, финансовых и пр.), вовлекаемых идеей для обеспечения своего существования в материальном мире.

В настоящем докладе показано, что процесс создания описывается функцией триединства. Он является процессом перехода от замысла (идеи) через технологии к материальному объекту, включая акт материализации, существование и дематериализацию объекта-носителя идеи. Таким образом, можно говорить о триединстве процесса создания как материальном воплощении идеи и образа объекта.

Открытым остается вопрос о механизмах возникновения идеи, в т.ч. как результате творчества, и способах интенсификации этого процесса. Интересным аспектом рассматриваемой модели является и вопрос о путях движения идеи к цели, об особенностях ее распространения, о влиянии идеи, в материальном воплощении, на окружающие объекты.

Необходимым условием распространения и материального существования идеи является наличие соответствующей среды (канала).

Показано, что идея может целенаправленно формировать такую среду. Простейшими средами передачи информации для распространения идеи являются, например, радиоканал; сеть Интернет, включая физические среды передачи информации, протоколы и алгоритмы ее передачи и обработки; интегрированная информационная среда в CALS-технологиях; организация социальных групп и пр.

Дискуссионным остается вопрос о жизни идеи в других материальных и идеальных объектах, в том числе, после достижения цели создания или после дематериализации (распада) объекта-носителя идеи.

Детально рассмотрены два механизма создания [Lysenko V.A. Information basics of creation // Материалы международной конференции "Региональная информатика - 2012", СПб, СПОИСУ – 2014, с. 340]: когда Создатель (инженер, программист, дизайнер, художник, поэт, природа и т.д.) планирует и строго контролирует материализацию идеи и когда материализация предварительно

запрограммирована и допускает определенную степень свободы во время этого процесса (например, при кодировании и передаче генетической информации, в алфавитах, при передаче информации с использованием финансовых инструментов; при самосборке, при самоорганизации, и пр.). Также раскрыты особенности целеполагания в создании: с четко или нечетко определенными целями или нечетко определенным образом будущего материального объекта-носителя идеи.

Особо отмечено, что при анализе и моделировании процессов создания необходим сбалансированный подход к роли и взаимодействию информации (идеи) и ее материального воплощения.

Проанализирована связь теории создания с такими научными дисциплинами как математика, общая теория систем, кибернетика, информатика и др. Показана роль теории создания для разработки наукоемких технологий и различных классов [Информационные технологии в дизайне [Электронный ресурс: http://itd-ri.ru/Scientifichighlights.htm] объектов проектирования.

Научные положения теории создания использованы при разработке и внедрении новых информационных систем и перспективных композиционных материалов функционального назначения.

Павловская О.В., Дроздова Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна

ОСОБЕННОСТИ РЕДИЗАЙНА САЙТОВ

При быстром развитии современного мира все так же быстро устаревает. Необходимо все время подстраиваться под новые условия. Это касается и бренда различных компаний. Рано или поздно его необходимо будет обновить, каким бы он не был заметным и популярным, его известность может превратиться в избитость. Бренд также должен соответствовать времени, находиться в постоянном развитии, иначе он может стать приевшимся и скучным. Такие проблемы решает ребрендинг. Так как основную информацию о компании несет в себе ее сайт, а внешний вид оценивается пользователем исходя из фирменного стиля и логотипа компании, то вышеперечисленные презентационные составляющие в первую очередь требуют редизайна и модернизации.

Ребрендинг — это изменение бренда, либо его составляющих (названия, логотипа, фирменного стиля), с комплексом необходимых для этого мероприятий.

Редизайн – это модернизация дизайна ресурса компании, проведение доработки необходимых графических элементов или создание абсолютно нового дизайна, если в этом есть необходимость фирменного стиля заказчика.

Модернизация и редизайн сайта необходимы, когда требуется обновление интерфейса, добавление новых веб-сервисов, переход на другую платформу, увеличение эффективности работы веб-ресурса разрыв отношений с предыдущими разработчиками, изменение маркетинговой стратегии компании, смена направленности ресурса и его целевой аудитории, увеличение уровня конверсии посетителей в клиентов и т.д.

Редизайн сайта должен осуществляться по особым правилам. В процессе модернизации сайтов рассматриваются такие возможности как: смена интерфейса, подстройка под мобильные версии, частичная модернизация, изменение программной части проекта, полная переделка, перенос системы на Битрикс, SEO-оптимизация, редизайн айдентики – набора элементов стиля компании и т.д. Таким образом, используя современные технологии можно создать качественный сайт, хорошо оформленный, многофункциональный, удобный и прибыльный для компании.

Приданов П.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ АВТОМАТИЧЕСКОЙ ПЛАНИРОВКИ ИНТЕРЬЕРА

Обустройство и уют собственного жилья является важным и волнующим вопросом для многих. Особенно это актуально, когда люди переезжают в совершенно новое для них место жительства.

Сегодня существует множество фирм, которые готовы за немалые деньги предложить “уникальные” решения для будущего интерьера.

Проблема данного способа - это большие затраты, как денежных средств, так и времени на реализацию. Человеку необходимо звонить, договариваться, ездить на встречи в офис, обсуждать наброски и черновые варианты. Конечно, результат данного способа в большинстве случаев оправдывает затраченные средства, но не все готовы платить большие деньги, а у кого-то просто нет времени.

Так же существуют многочисленные конструкторы интерьеров, где пользователю предоставляют возможность самому из готовых библиотек мебели собрать интерьер. Например, Autodesk Homestyler. Проблема данного способа обусловлена тем, что люди зачастую даже не

представляют, что они хотят видеть в своем будущем интерьере и вопрос о создании интерьера с нуля заводит их в тупик. Еще одна проблема данного способа - последующая визуализация созданных ими интерьеров. В большинстве подобных программ визуализация созданного интерьера имеет достаточно условный и схематичный вид.

Третий способ самый простой и популярный - это выбор своего варианта из уже готовых интерьеров. Пользователь просматривает фотографии пока не найдет то, что ему понравится. Проблемой данного способа является отсутствие индивидуальности и гибкости.

В картинке выбранного интерьера человек не может ничего изменять. Например, цвет стен, расположение мебели, освещение чтобы посмотреть, как это будет выглядеть в реальности.

Универсальным решением может стать разработка программы, которая будет создавать интерьер автоматически, основываясь на предпочтениях пользователя.

Человек выбирает размеры своей комнаты, количество необходимой мебели, источников света и цветовой колорит, своего будущего интерьера.

Программа выбирает случайным образом мебель, обои, пол и т.д. из собственной библиотеки и создает случайный интерьер, основываясь на введенных пользователем критериях. Расположение мебели и освещение программа выбирает самостоятельно, основываясь на заложенных в нее скриптах.

Преимуществом данного метода является простота, вариабельность и универсальность. Пользователь выбирает необходимые ему критерии, а затем нажимаем одну кнопку, до тех пор, пока ему не понравится предложенный результат. Благодаря огромной библиотеке готовых элементов, программа способна предложить множество вариантов.

Подкорытов С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МОДЕЛИРОВАНИЕ ГЛАДКИХ САМОПОДОБНЫХ ПОВЕРХНОСТЕЙ

Одним из важнейших направлений развития компьютерных систем автоматизированного проектирования (Computer Aided Design System) является совершенствование их инструментов моделирования.

В современных системах автоматизированного проектирования широко используются итеративные методы моделирования. В основе данных методов лежит принцип сходимости итеративных алгоритмов.

Для каждой исходной конфигурации контрольных точек (control points) итерации применения алгоритма сходятся к единственному предельному положению. Преимуществом данного подхода является возможность редактирования финального объекта с помощью изменения стартовой конфигурации контрольных точек.

Широким распространением пользуются алгоритмы, принадлежащие к классу subdivision schemes, используемые для моделирования кривых и двумерных поверхностей. Примерами таких алгоритмов являются схемы Ду-Сабина, Катмулл-Кларка, Лупа и другие. Данные схемы дают возможность описывать кусочно-полиномиальные кривые и поверхности. Однако применимость подобных схем ограничена тем, что определенные схемы могут применяться только лишь к конкретным конфигурациям контрольных точек, а так же необходимостью увеличивать количество контрольных точек ради увеличения детализации моделируемых объектов.

Голдман и др. показали, что объекты, описываемые подобными алгоритмами, обладают свойствами самоподобия. Это позволяет объединить вышеописанные методы с моделями, опирающимися на свойство самоподобия, тем самым позволяя моделировать не только кусочно-полиномиальные кривые и поверхности.

Моделирование объектов с использованием самоподобия впервые было предложено в виде Системы Итерированных Функций (Iterated Function System).

Впоследствии были предложены способы описывать самоподобные объекты с заданной топологической структурой Грань-Ребро-Вершина. При этом каждый элемент топологической структуры может быть оснащён набором контрольных точек, позволяющим управлять его геометрической формой отдельно от топологии. Использование такого подхода к моделированию кусочно-полиномиальных кривых и поверхностей позволили, в частности, решить проблему соединения различных subdivision schemes.

Известно, что схемы Ду-Сабина, Катмулл-Кларка и д.р. описывают поверхности с определёнными классами гладкости. Поскольку моделирование поверхностей с заданной гладкостью является важной инженерной задачей, то важно получить подобные результаты и для моделирования с использованием Систем Итерированных Функций.

Результат данной работы – вывод необходимых и достаточных условий существования касательных пространств к самоподобным поверхностям, описываемым с помощью Систем Итерируемых Функций.

Тимофеева Е.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ВЕРСТКА ГАЗЕТЫ В ИНТЕРНЕТЕ

Часто бюджетные организации, которые хотели бы иметь свое печатное издание и делиться актуальной и полезной информацией с коллективом не могут позволить себе оплатить работу верстальщика, а сами не имеют знаний в области верстки и дизайна, поэтому очень остро нуждаются в понятном и простом способе, с помощью которого можно создать свою собственное издание. Таким изданием может стать газета, сверстанная с помощью шаблонов, где есть готовые макеты и художественное решение.

В качестве интерфейса пользователя используется разработанное новая интернет-технология в виде веб-приложения. Веб-приложение с интерактивными шаблонами для верстки малобюджетной газеты популярно и интересно различному пользователю, благодаря достоинствам веб-приложения и простоте в обращении с шаблонами.

При разработке интерфейса веб-приложения был использован Twitter Bootstrap Framework 3.1.1. − интуитивно понятный и мощный интерфейс для быстрой и легкой разработки клиентской части веб-приложения, который облегчает разработку большого программного проекта. Включает в себя HTML и CSS шаблоны оформления для типографики, веб-форм, кнопок, меток, блоков навигации и прочих компонентов веб-интерфейсов, включая JavaScript расширения.

Одной из основных функций веб-приложения является возможность без профессионального программного обеспечения получить готовую газету.

Разработка новой интернет - технологии, выполняет следующие функции:

- Верстает газету с готовым дизайнерским решением;
- Сохраняет шаблоны в PDF файл;
- Интерактивно управляется пользователем без специальных знаний и правил допечатной подготовки;
- Работает без профессионального программного обеспечения, достаточно наличие только Интернет браузера;
- Имеет рекомендации по верстке текста и иллюстраций.

При разработке пользовательского интерфейса веб-приложения для верстки газеты по шаблону, особое внимание уделялось простому дизайну с максимально понятным управлением

Одним из важных пунктов меню являлись «Шаблоны», которые содержат выпадающий список для выбора темы макета для верстки. Темы очень разнообразны: школьная газета, районная газета, детская, газета о красоте и здоровье.

С появлением новых технологий, актуальность печати газет и журналов сейчас по-прежнему остается очень высокой. А значит, разработанное веб-приложение для верстки малобюджетной газеты по шаблону будет популярно. Уникальность интерактивного приложения в том, что оно бесплатное и не имеет аналогов в Интернете. Им может воспользоваться любой пользователь, которого оно заинтересует.

Трубникова А.М., Кузнецова Л.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна

ПРОБЛЕМЫ СНИЖЕНИЯ ЭФФЕКТИВНОСТИ ПОИСКА И ОБРАБОТКИ ИНФОРМАЦИИ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

Сегодня, благодаря возможностям сети Интернет пользователь получает доступ к огромному количеству информации, что, безусловно, предоставляет широкие возможности для решения творческих, профессиональных и других задач. Однако, кроме положительных аспектов интенсивного увеличения доступной информации в сети, существуют и отрицательные стороны, связанные как со сложностью поиска, так и обработки полученной информации.

Одной из проблем здесь является несовершенство поисковых систем и отсутствие у пользователя навыков грамотного составления запроса. Также негативно сказывается особенность Российских поисковых систем, связанная с несоответствием кодировки на компьютере пользователя и искомого сайта. Это приводит к появлению информационного шума при поиске и ограничению доступа к уже имеющейся полезной информации.

Другая проблема – всё возрастающие объёмы и гипертекстовая организация информации в сети Интернет. Это приводит к тому, что утрачивается способность пользователя читать тексты большого размера, самостоятельно обрабатывать и осмысливать значительные объемы данных. Кроме того, гипертекстовый формат также способствует упрощению и поверхностному изучению материала без детального его освоения; чтение становится нелинейным. Пользователь чаще имеет дело с внешними носителями информации, что затрагивает механизмы работы памяти и внимания; к участию в мыслительных процессах присоединяются различные электронные устройства. В целом

это негативно влияет на эффективность анализа и восприятия информации, а главным критерием поиска становится скорость получения, а не её качество.

Для преодоления существующих ограничений возможен ряд мер. В первую очередь, пользователю необходимо разобраться, как устроены и по каким принципам функционируют основные инструменты для поиска информации в Глобальной сети, знать, какие языки запросов нужно применять в той или иной ситуации. Во-вторых, необходимо овладение методиками чтения и фильтрации, умение отбирать ценное и полезное, пользуясь эффективными алгоритмами анализа и смыслового восприятия текста, что позволит сократить временные и интеллектуальные затраты на поиск информации.

Чеботарева И.Б., Чеботарев Р.И., Муравьева А.В.
Украина, г. Харьков, Харьковский национальный университет радиоэлектроники

КОМПЛЕКСНАЯ ОЦЕНКА УРОВНЯ КАЧЕСТВА ФЛЕКСОПЕЧАТИ ТУБНОЙ УПАКОВКИ

С момента своего появления на рынке, тубная упаковка завоевала популярность как потребителей, так и производителей различных товаров. Тюбик незаменим для зубной пасты, кремов, бальзамов, а также для многих пищевых продуктов. Упаковка в виде тубы удобна и практична, способна придать продукции прекрасный внешний вид. Поэтому предприятия, которые занимаются тубной упаковкой, придают большое значение вопросам качества выпускаемой продукции.

В качестве объекта исследования выбрано предприятие ООО «Тубный завод» (г.Харьков). Это крупнейшее предприятие Украины по производству тубной упаковки. Для повышения эффективности контроля качества печати тубной упаковки было принято решение разработать такой комплексный показатель качества, который будет учитывать основные параметры, влияющие на качество печати.

Контроль данного вида продукции на предприятии выполняется только визуальными методами. Комплексная оценка качества печати связывает визуальную оценку, инструментальную оценку и физические показатели качества оттиска, полученного с помощью флексопечати.

Для количественной оценки необходимо определить основные параметры, которые влияют на качество печати, они и являются единичными показателями качества, которые могут быть количественно определены в процессе печати.

Для данной задачи было принято решение использовать упрощенную схема комплексного анализа. Для этого определены следующие исходные данные для эксперимента: вид продукции – туба экструзионная; способ печати – флексографский; цвет пластика – белый.

Основными единичными показателями являются: 1) растискивание – процент прироста относительной площади растрового элемента; 2) неприводка (несовмещение красок) – микрометры, относительно черной краски; 3) изменение общего контраста, выраженное изменением оптической плотности; 4) отклонение по цветам (величина цветового различия) – расхождение между исходными Lab координатами цвета и полученными при печати.

Эталонные (базовые) и граничные значения этих параметров были определены, исходя их требований нормативной документации (отраслевые стандарты и технические задания на тубную продукцию, разработанные на предприятии).

Следующим этапом является формирование комплексного показателя качества печати, который является функцией от единичных показателей с заданными весовыми коэффициентами.

Для определения коэффициентов весомости был проведен экспертный опрос. Основная задача при выборе членов экспертной группы заключается в привлечении специалистов отрасли, способных максимально точно решить поставленную задачу. Были выбраны семь экспертов, которые непосредственно связаны с производством упаковки и хорошо владеют вопросами оценки и контроля качества полиграфической продукции: 1 – технолог (флексопечать); 2 – инженер по допечатной подготовке (флексопечать); 3 – инженер по качеству (флексопечать); 4 – директор предприятия (флексопечать); 5 – главный инженер (флексопечать); 6 – печатник (флексопечать); 7 – инженер-технолог (изготовление флексоформ).

Для оценки согласованности мнений экспертов был определен коэффициент конкордации, равный 0,92, что подтверждает хорошую согласованность экспертов. Для определения согласованности по отдельным показателям были оценены коэффициенты вариации для каждого из них. Все показатели были не ниже среднего, т.е. экспертный опрос состоялся и определенные весовые коэффициенты можно использовать для формирования и расчета комплексного показателя.

Проанализируем значения полученных коэффициентов весомости. Самым значимым (0,33) является соблюдение необходимого растискивания – основное требование к качеству флексопечати. Это во многом объясняется спецификой флексопечати (гибкие формы, невпитывающий материал) и необходимостью жесткого выполнения всех технологических режимов. Вторым по значимости (0,26) является правильное воспроизведение цветов, т.к. это напрямую влияет на качество готовой продукции и мнение заказчика. При печати тубной упаковки, несмотря на незначительное ослабление требований к несовмещению красок (0,2 мм для туб и 0,1 для пленок), этот параметр, по мнению экспертов, также важен (0,24). Меньше внимания при оценке качества, по мнению членов экспертной

группы, стоит уделять контрасту изображения, т.к. при правильном технологическом процессе (правильный выбор красок, лаков и пр.), изображение и так получается насыщенным и контрастным.

Рассмотренные основные показателя можно контролировать инструментальными методами в процессе печати и на основании полученных данных проводить оценку уровня качества с помощью разработанного комплексного показателя. Процедура расчета комплексного показателя реализована в MS Excell. В дальнейшем можно доработать данную процедуру для обработки потока измеренных данных в автоматическом режиме. Использование комплексного показателя качества на производстве позволит автоматизировать процесс принятия решения об уровне качества продукции, что упростит операцию контроля качества, устранит ошибки визуального контроля и в целом ускорит процесс производства продукции.

Чеботарева И.Б.
Украина, г. Харьков, Харьковский национальный университет радиоэлектроники

ФОРМИРОВАНИЕ НЕЧЕТКИХ ОЦЕНОК ХАРАКТЕРИСТИК ЦИФРОВЫХ ОРИГИНАЛОВ

На основе современных методов анализа изображений можно эффективно решать многие проблемы в полиграфической отрасли. Обычно полиграфические предприятия получают уже готовые макеты полиграфической продукции, но в настоящее время, когда идет борьба за каждого заказчика, небольшие предприятия могут работать и с исходными, почти не обработанными изображениями. Например, когда готовятся большие печатные каталоги или срочно печатаются цифровые фотографии. Поэтому возникает большая группа ошибок, связанная с исходными дефектами изображений (шум, нечеткость, неправильное разрешение или размер и т.п.). Если формализовать процедуры проверки и оценки цифровых оригиналов, то можно разработать процедуры автоматического улучшения полученных оригиналов и автоматизировать данный этап допечатной подготовки. Для этого необходимо решить задачу классификации искажений (ошибок) цифровых оригиналов, которые в большинстве случаев невозможно оценить объективно численными методами.

При анализе изображений выделяют объективные и субъективные характеристики. Объективные характеристики – это атрибуты изображений, которые связаны с природой зрительного восприятия, представлением и обработкой цифровых изображений на компьютере.

Субъективные оценки выражаются в форме лингвистических переменных. Каждый атрибут изображения можно описать с помощью лингвистической переменной, которая принимает определенное значение, характеризующее качество изображения.

Для решения задачи формирования нечетких оценок характеристик цифровых изображений были проанализированы и выделены основные атрибуты изображений, важные при репродуцировании. Каждый атрибут является лингвистической переменной, которая принимает определенное значение (терм), характеризующее качество изображения. Например, Т «Резкость» = {РЕЗКОЕ, НЕМНОГО РАЗМЫТОЕ, ОЧЕНЬ РАЗМЫТОЕ}, Т «Общая светлота» = {ОЧЕНЬ ТЕМНОЕ, ТЕМНОЕ, СРЕДНЕЕ, СВЕТЛОЕ, ОЧЕНЬ СВЕТЛОЕ} и т.д.

Решение задачи формирования терм-множеств для лингвистических переменных предлагается осуществить в несколько этапов:

a) подготовить тестовый набор изображений с учетом пожеланий полиграфических предприятий;

b) выполнить количественный анализ характеристики изображений расчетными методами для получения множества значений базовых переменных;

c) сформировать терм-множества для каждой лингвистической переменной;

d) выполнить субъективный анализ изображений наблюдателями-экспертами;

e) сравнить оценки изображений, полученные количественными и субъективными методами и выяснить, какой из количественных методов наиболее точно характеризует качество изображений;

f) определить нечеткие границы;

g) используя нечеткие границы, полученные в результате экспертного оценивания, построить функции принадлежности для каждого терм-множества лингвистических переменных;

h) получить уточненные интервалы значений базовых переменных.

Основными лингвистическими переменными являются: «Размер изображения», «Разрешение изображения», «Контрастность», «Общая светлота», «Резкость», «Шумы и помехи», «Детальность». Соответствующими базовыми переменными являются: «Площадь», «Разрешение», «Двумерный градиент», «Математическое ожидание», «Дисперсия для ч/б изображений», «Степень размытия», «Усредненная энтропия». Для каждой лингвистической переменной был определен набор термов и базовые переменные, позволяющие количественно оценить лингвистические переменные.

Формирование исходной информации для построения функций принадлежности выполняется методом группового опроса экспертов. В данной работе предложен метод «Дельфи». Он предусматривает проведение экспертного опроса в несколько туров. Процесс выработки суждений экспертами управляется через обратную связь. К участникам обращаются с просьбой не только высказать свои мнения, но и привести их обоснование. Процесс продолжается до тех пор, пока

несовпадения точек зрения становятся незначительным. После этого фиксируются полученные значения. Полученные результаты используются для построения функций принадлежности терм-множества соответствующей лингвистической переменной.

Разбивая шкалу значений базовых переменных на интервалы, процесс оценки качества изображений становится автоматизированным при последующем анализе изображения. Таким образом, формируется целая система показателей, которые характеризуют качество оригинала на этапе допечатной подготовки, и количественно отражают степень близости показателя к предельным значениям. Построенные функции принадлежности, количественно характеризующие лингвистические переменные, позволяют формализовать нечеткую базу знаний для принятия решений в задаче классификации искажений цифровых оригиналов. Полученные результаты могут быть использованы при разработке автоматизированных процедур улучшения качества изображений.

Шефер Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет промышленных технологий и дизайна, Высшая школа печати и медиатехнологий

КОМПЕНСАЦИЯ ВЛИЯНИЯ ДЕФЕКТОВ ФОРМЫ ПЕЧАТНЫХ ЦИЛИНДРОВ НА РАСТИСКИВАНИЕ ПУТЕМ ИЗМЕНЕНИЯ РАЗМЕРОВ РАСТРОВОЙ ТОЧКИ НА ДОПЕЧАТНОЙ СТАДИИ

Полиграфическое оборудование за последние годы постоянно совершенствуется, происходит модернизация производства, увеличивается скорость работы машин. При этом немаловажным фактором остается качество конечного продукта. Для того, чтобы уменьшить время получения конечного продукта необходимо учитывать ряд факторов, влияющих на скорость и качество печатного процесса.

Точное воспроизведение цвета в процессе печати изображений обеспечивается различными показателями, наиболее важным и обобщающим из которых является растискивание растровых точек. Электронный макет изображения состоит из множества идеальных округлых точек, диаметр которых обеспечивает передачу нужного полутона. При переносе на носитель (бумагу) точки увеличиваются в размерах и принимают неправильную форму. Такое явление приращения площади растровой точки и получило название растискивание. Поскольку растискивание следует относить к особенностям системы «офсетная машина – краска – бумага», то его избежать невозможно, но вполне реально обеспечить его стабильность и компенсировать на этапах подготовки печатной формы и непосредственно во время печати.

Радикальным методом повышения производительности и снижения технологических потерь в полиграфии является способ предугадывания растискивания растровых точек, что позволяет значительно снизить трудовые и материальные издержки производства печатной продукции.

На изменение размера точки влияет много факторов. Причины растискивания, источником которого является печатное оборудование и условия печати, целесообразно детализировать по следующим факторам:

- давление между механическими парами в процессе печати;
- различие линейных скоростей офсетных цилиндров в рулонных машинах, различие диаметров офсетных и печатных цилиндров в листовых машинах;
- механический износ поверхности печатного цилиндра, приводящий к изменению его формы (бочкообразность, «приталенность» и др.);
- размер и форма печатного элемента: круглая точка имеет наименьшее растискивание при прочих равных условиях.

При реальном выполнении печати регулирование размера точки выполняется путем получения пробных оттисков, на которых проверяется уровень полученного растискивания. Это достаточно затратный технологический метод, в процессе которого увеличивается время на приладочные работы и расходуется бумага и краска. Для того, чтобы отойти от этого метода и компенсировать растискивание еще на стадии допечатной подготовки, предлагается промоделировать этот процесс средствами программирования, а полученную модель использовать при подготовке электронного макета. Зная параметры изменения формы печатного цилиндра, можно в программе построить кривую, отображающую величину растискивания на отдельных участках изображения. После этого можно будет вносить изменения в размер растровых точек, согласно полученным данным, еще до процесса печати.

Модель растискивания и процедура построения кривой, моделирующей дефект печатного цилиндра, выполнена в системе программирования Matlab. В модели каждый пиксель растрового цифрового изображения представляется в виде квадрата состоящего из NxN элементов, т.е. число, обозначающее яркость пикселя, заменяется матрицей. Для моделирования эффекта растискивания количество элементарных квадратов каждого пикселя исходного изображения меняется на некоторую величину ΔN.

Использование алгоритма, учитывающего увеличение или уменьшение растровой точки, позволяет снизить производственные издержки и повысить рентабельность выпускаемой продукции.

Эрштейн Л. Б.
Россия, Санкт-петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского университета промышленных технологий и дизайна

РАЗРАБОТКА ДИЗАЙНА ИНТЕГРИРОВАННОГО ИНТЕРФЕЙСА КАК СПОСОБ ОПТИМИЗАЦИИ РАБОТЫ ПОЛЬЗОВАТЕЛЯ С БАЗОЙ ДАННЫХ

Одним из наиболее распространенных типов программного обеспечения для современных компьютерных устройств в настоящее время являются базы данных. Фактически нельзя представить себе не одного предприятия ни в какой области деятельности, которое не использовало бы в своей работе какую-либо базу данных.

Одним из наиболее значимых элементов любой базы данных, по какой бы технологии она не была спроектирована, является интерфейс. Вопросу разработки интерфейса баз данных, уделяли внимание многие исследователи [1, 2, 3]. Однако конкретных требований к нему в исследованиях сформулировано не было. Учитывая тот факт, что конечный пользователь имеет дело именно с интерфейсом базы данных, проектирование дизайна интерфейса имеет существенное значение. Работа с недостаточно удобным интерфейсом будет приводить к значительным временным потерям, а значит, по сути, уменьшать эффективность деятельности компаний, поэтому формулировка конкретных требований к дизайну интерфейса баз данных является актуальной проблемой развития современных информационных технологий.

Рассмотрим принципы реализации интерфейса каждой из основных функций интерфейса базы данных.

1. Функция ввода. Наиболее удобным для ввода является ввод данных в таблицу, так как переключение между полями, не требует дополнительных операций, как в случае использования текстовых полей. Кроме того, ввод в таблицу позволяет отслеживать правильность введенных данных целиком, что, в случае текстовых полей является затруднительным, поэтому ввод данных в таблицу является более предпочтительным, чем в текстовые поля.

Вторым моментом является использование выпадающих списков фиксированных значений в процессе ввода данных. Необходимо исключить полный ввод любых повторяющихся многократно данных. Такой способ ввода позволяет экономить большое количество времени и сил. Опыт показывает, что через выпадающие списки иногда можно вводить до половины содержимого баз данных, в зависимости от специфики и особенностей конкретной ситуации.

Переключение между таблицами ввода должно быть как при помощи указателя мыши, так и при помощи горячих клавиш. Все таблицы, по возможности должны быть на одном экране, а в случае не возможности этого, должен присутствовать элемент управления, предназначенный для возвращения на предыдущий экран. Категорически необходимо избегать горизонтальной полосы прокрутки при вводе данных, при этом (как уже упоминалось) вертикальная полоса присутствовать может.

2. Функция редактирования. Редактирование данных желательно осуществлять прямо из таблицы ввода. Процесс редактирования должен предусматривать возможность выделения нескольких или одного поля в любом сочетании, как с использованием горячих клавиш, так и указателя мыши. Редактирование должно позволять удалять или изменять любые введенные ранее данные (если иная ситуация не предусматривается заранее).

3. Вывод. Каждая операция вывода должна быть снабжена соответствующей понятной подписью, из нее должно следовать, что пользователь получит в результате ее применения. Желательно группировать все функции вывода, на странице, предназначенной для ввода информации, при этом, сами функции могут быть реализованы как при помощи гиперссылок, так и при помощи кнопок.

В том случае если, не существует возможности поместить функции вывода на одном экране, на котором располагается ввод, можно создать общую страницу для управления выводом информации, при этом на этой странице должен присутствовать элемент управления, позволяющий вернуться на страницу ввода.

Таким образом, разрабатывается общий интегрированный интерфейс базы данных, позволяющий реализовать все функции базы данных на одном или минимально возможном количестве экранов.

Такая реализация дает возможность существенно оптимизировать работу с базой данных, за счет того, что использование базы осуществляется с минимальным количеством операций. То есть для того чтобы выполнить ту или иную необходимую функцию, нужно использовать элементы управления компьютерным устройством как можно меньшее количество раз.

В результате можно утверждать, что разработка интегрированного интерфейса баз данных, позволит повысить эффективность деятельности компаний, за счет экономии времени и сил, конечных пользователей баз данных, так как работа с базами с которыми существенную часть бизнес процессов практически любой фирмы.

ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ

Вавилов С.А., Лытаев М.С.
Россия, Санкт-Петербург, ЗАО «СПИИРАН-НТБВТ»

КАЛИБРОВКА И ВАЛИДАЦИЯ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ ЗОН ВИДИМОСТИ РЛС В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

Задача оперативного прогнозирования и диагностики зон обнаружения целей РЛС в постоянно изменяющихся метеорологических условиях является актуальной проблемой морской и наземной радиолокации. Хорошо известно, что пространственные изменения индекса преломления тропосферы способны оказывать существенное влияние на распространение радиоволн в СВЧ диапазоне. Использование математического моделирования позволяет предсказать предельные зоны действия радаров для обнаружения различных объектов в зависимости от текущих условий в реальном времени. Развитие современных геоинформационных систем дает возможность эффективно собирать и обрабатывать большие объемы геопространственных данных, а также обеспечивает наглядное представление полученных результатов моделирования.

Анализ существующих систем прогнозирования распространения электромагнитных волн, в том числе таких как соответствующее программное обеспечение стран участников НАТО: AREPS и PETOOL, показывает, что они обладают серьезными недостатками. В частности, хорошо известно, что метод расщепления Фурье, используемый в подобных системах при численном решении задачи по методу параболического уравнения, в силу вынужденного искусственного ограничения области интегрирования, дает ложные отражения от верхней границы расчетной области, что существенно сокращает максимальную дальность прогнозирования и увеличивает допустимый диапазон ошибок в определении электромагнитного поля. Введение искусственного поглощающего слоя вблизи верхней границы расчетной области способно на несколько порядков уменьшить влияние ложных отражений, однако его эффективность зависит от конкретных параметров излучающей антенны, ландшафта и коэффициента преломления среды. Кроме того, параметры самого слоя определяются не строго, а исходя из некоторых эмпирических соображений и, таким образом, требуют калибровки и верификации. Следовательно, существует необходимость в разработке метода расчета функции ослабления в близи поверхности Земли в неоднородной среде, не требующего введения искусственного поглощающего слоя, отдельного рассмотрения широкоугольного и узкоугольного приближения, а также способного работать в узком диапазоне допустимых ошибок.

Выполнено исследование задачи распространения электромагнитных волн в параксиальном приближении, отвечающей плоской геометрии. Источник излучения задается своей диаграммой направленности. Осуществляется редукция исходной задачи к построению решения уравнения Гельмгольца с объемным источником в его правой части. Указанный источник определяется из решения интегрального уравнения Фредгольма первого рода. Полученное решение является устойчивым относительно исходных данных. На множестве функций ограниченной вариации может быть построено его квазирешение. Для учета произвольной структуры тропосферы на распространение электромагнитных волн высокой частоты, вводится в рассмотрение интегральное уравнение Фредгольма второго рода относительно образа Фурье, отвечающего искомой функции ослабления, которое в случае, когда функция индекса преломления финитна, поддается эффективному численному решению методом квадратур. В ходе численной реализации предложенного метода был разработан адаптивный метод высокоточного вычисления обратного преобразования Фурье от функции ослабления, основанный на аппроксимации образа Фурье полиномами Чебышева произвольного порядка.

Таким образом, в отличии от метода параболического уравнения, предлагаемый подход позволяет, оставаясь в рамках параксиального приближения, решать исходную задачу без введения понятия узкоугольного или широкоугольного приближения. Кроме того, данный метод позволяет в рамках приближения «плоской земли» при построении численного решения обходиться без искусственно вводимого понятия поглощающего слоя. Предложенная численная схема не требует ручного подбора каких-либо расчетных параметров, размеры сетки по продольной переменной и по высоте выбираются исключительно из требований визуализации и не влияют на точность расчетов.

Следует отметить, что несмотря на эффективность разработанных численных алгоритмов, скорость работы метода расщепления Фурье при правильно подобранных параметрах расчетной сетки и поглощающего слоя в несколько раз превосходит предложенный метод. Таким образом алгоритмы, основанные на пошаговом решении параболического уравнения, остаются единственно пригодными для оперативного прогнозирования в реальном времени. Однако ввиду невозможности

контроля точности решения в упомянутых методах, предложенный подход оказывается весьма полезным при подборе расчетных параметров в зависимости от различных входных данных, проведении калибровки и верификации имеющихся оперативных систем прогнозирования. Кроме того, предложенный метод может применяться в задачах, где требуется высокая гарантированная точность вычислений, например при расчете энергетических характеристик наземных РЛС или при планировании и анализе результатов экспериментов.

Волгин П.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ МОНИТОРИНГА МОРСКОЙ ОБСТАНОВКИ

При организации проектирования и создания систем мониторинга морской, управлении ими в процессе функционирования и развития возникает проблема обоснованности и эффективности принимаемых решений. Применение для обоснования решений, планов и для управления процессом их реализации существующих методов объективной оценки способно значите

льно повысить эффективность и качество функционирования организационно-технических систем. В современных условиях в качестве одного из основных методов исследования закономерностей, присущих функционированию систем мониторинга, широкое распространение получило математическое моделирование.

Важнейшими особенностями, характерными для условий принятия решения, и, прежде всего, в сфере мониторинга морской обстановки и контроля за морской деятельностью, является острый дефицит времени, необходимость тесного взаимодействия с другими информационными системами, а, зачастую, и наличие активной противоборствующей (конкурирующей) стороны. Именно поэтому для исследования и выявления закономерностей присущих процессу мониторинга и контроля обстановки и деятельности в морской зоне прибегают к использованию имитационного моделирования.

Для реализации процесса имитационного моделирования структурно-функциональную модель, являющуюся основой имитационной модели, необходимо дополнить параметрами, данными, описывающими детали функционирования системы в пространстве, в различных средах и во времени, используя логико-математическую форму представления имеющихся взаимосвязей и взаимозависимостей.

Применение геоинформационных технологий позволяет резко увеличить оперативность и качество работы с пространственно - распределенной информацией.

Интегрированная имитационная модель системы мониторинга обстановки в морской зоне предусматривает реализацию интеграционной функции результатов имитационного моделирования (текущих и итоговых, в пространстве моделирования и во времени реализации процесса) в различных средах пространства мониторинга, в сочетании с информацией, предоставляемой геоинформационной системой.

Целью такой интеграции является возможность учета в модели взаимно обуславливающих факторов обстановки при нахождении различных объектов наблюдения в различных средах, прогнозировании изменений в обстановке и обеспечение процесса принятия обоснованного решения на основе мониторинга различных сред контролируемой зоны в динамике изменения обстановки.

Главными возможностями, предоставляемыми геоинформационной системой (ГИС), являются пространственная и временная интеграция используемых данных, а также необходимый уровень визуализации реализуемого процесса. При этом новое качество решение проблемы гармонизации, интеграции и слияния данных в интегрированной имитационной модели системы мониторинга в целом может быть обеспечено интеллектуальной ГИС, которая предусматривает использование, наряду с традиционной ГИС-технологией включением в ее состав методов и средств искусственной интеллектуальности.

Методы имитационного моделирования, современные информационные технологии могут быть главной основой при создании специального программного обеспечения сложных, пространственно распределенных, динамических систем, к которым, в том числе, относятся системы мониторинга и контроля морской обстановки, а также являться мощным и эффективным средством исследования.

Применение имитационного моделирования позволяет исследовать объекты, реальные эксперименты над которыми затруднены или невозможны (дорого, опасно для здоровья, однократные процессы, невозможные из-за физических или временных ограничений – находятся далеко, еще или уже не существуют и т.п.).

Применение для целей имитационного моделирования интеллектуальных ГИС дает возможность повысить эффективность функционирования различных систем, описываемых соответствующими имитационными моделями, в том числе связанных с принятием решений, отвечающих за безопасное развитие пространственных процессов морской деятельности.

Ермолаев В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЕ ИНТЕЛЕКТУАЛЬНЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ПРОЕКТИРОВАНИИ ГИДРОАКУСТИЧЕСКИХ СРЕДСТВ

При разработке гидроакустических средств (ГАС), широко используются системы автоматизированного проектирования (САПР). Такие системы должны обеспечить как моделирование всех процессов многоуровневой обработки информации гидроакустическими средствами, так и возможность синтеза структуры проектируемой ГАС и алгоритмов ее функционирования. Поэтому в состав САПР ГАС, как правило, входят две подсистемы: имитационного моделирования и автоматизированного проектирования.

Имитация динамически изменяющейся модели обстановки, формирование соответствующей этой обстановке распределения акустического поля сигналов и помех на элементах гидроакустической антенны, а также реализация проектируемых алгоритмов обработки гидроакустической информации предполагает работу с геопространственными данными, характеризующими объекты моделирования и среду. Наиболее развитыми возможностями по решению таких задач обладают интеллектуальные географические информационные системы (ИГИС), сочетающих в себе возможности геоинформационных и экспертных систем.

Специальное программное обеспечение ИГИС, адаптированное к обеспечению функций САПР ГАС должно иметь трехуровневую клиент-серверную архитектуру и включать следующие компоненты.

А) Серверная часть:

- сервер объектов. Обеспечивает формирование модели предметной области и предоставляет клиентам данные и знания о предметной области;
- картографический сервер. Обеспечивает представление картографической информации, формирование картографических слоев, предоставление картографических данных;
- гидрометеосервер. Обеспечивает сбор, обработку и отображение текущих гидрометеорологических данных;
- сервис алгоритмов обработки данных. Представляет собой библиотеку математических методов, алгоритмов, процедур, обеспечивающих имитацию динамически изменяющейся обстановки, а также обработку данных текущей (фактической или моделируемой) обстановки;
- сервер бизнес-процессов. Обеспечивает реализацию бизнес-процессов, связанных с формированием структуры ГАС и с исследованием алгоритмов обработки гидроакустической информации;
- машина логического вывода и экспертная система. Предназначены для решения задач выработки рекомендаций по использованию гидроакустических средств и систем;
- сервер гидроакустических расчетов. Обеспечивает проведения расчетов передаточной функции двумерно-неоднородной среды;
- сервер внешних связей обеспечивает получение данных от внешних источников в согласованном формате, предоставляет внешним потребителям имеющиеся в программном комплексе данные и результаты их обработки.
- сервис администрирования предоставляет инструменты настройки программного комплекса и обеспечивает разграничение прав доступа пользователей к информационным ресурсам, а также позволяет изменять набор используемых для обработки алгоритмов и методов.

Б) Клиентская часть. Должна быть реализована в виде толстого клиента и включать следующие программные компоненты: ГИС-интерфейс, набор редакторов обеспечивающих формирование исходной обстановки моделирования, имитацию действий объектов и многоуровневую обработку гидроакустической информации.

В) Базы данных и знаний.

Г) Сеть обмена данными.

Приведенная архитектура и структура ИГИС обеспечивают весь спектр задач моделирования, обработки геопространственных данных, а также выработки управляющих воздействий в САПР ГАС.

Ивакин Я.А., Потапычев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ГЕОХРОНОЛОГИЧЕСКИЙ ТРЕКИНГ – СПЕЦИАЛИЗИРОВАННЫЙ ГИС-ИНСТРУМЕНТАРИЙ ИСТОРИЧЕСКОГО ИССЛЕДОВАНИЯ

Географические информационные системы (ГИС) сегодня являются эффективным инструментарием исследователей в гуманитарных науках, прежде всего в истории. Однако класс специализированных методов и ГИС-средств интеллектуальной поддержки исследователя при решении именно исторических задач, при проведении компьютерного моделирования тех или иных исторических процессов в геопространстве не достаточен. Как правило, такие исследования

базируются на использовании универсальной функциональности ГИС, т.е. на использовании геодезических, топографических и универсально-географических приложений. Геохронологический трекинг – это пример специализированного ГИС-инструментария для решения соответствующего класса исторических задач. Основным конструктивом предлагаемого ГИС-инструментария является механизм интеграции хронологических и геопространственных данных в виде геохронологического трека, реализующий современные информационные методы интеграции информации.

Исходя из энциклопедического понимания слова “трек” как ряда точек на траектории движения, вереницы событий, можно трактовать “Геохронологический трек” – как совокупность параметров (данных), описывающих ряд последовательных событий в жизни индивида (группы, некоторой исторической общности) с привязкой ко времени и месту появления этих событий. На географической карте такой трек будет представлять кривую соединяющую географические точки нахождения исторической личности (группы и пр.) с цвето-градиентной привязкой к хронологии событий. Соответственно, геохронологический трекинг – это процедура (метод, процесс) построения, обобщения и интерпретации совокупности геохронологических треков по статистически значимой, в исследовательском смысле, социальной группе, которое позволяет выявить новые факты и закономерности в развитии исторических процессов.

Разработка алгоритмических и программных механизмов построения и корректного отображения геохронологических треков на электронной карте для отдельных исторических личностей, членов малых социальных групп, а так же интеграции исторической и географической информации при обобщении составляет существо самостоятельного и многоэтапного междисциплинарного исследования.

Предлагаемый в данной статье подход к применению научно-методического аппарата геохронологического трекинга в исторических исследованиях, как специализированного ГИС-инструментария, объективно требует дальнейшей проработки и развития этого аппарата. Однако, наглядность его реализации и высокая результативность позволяют прейти к предварительному выводу о его широкой научно-исследовательской применимости.

Работа выполнена при поддержке РФФИ (проект №16-07-00127).

Прокаев А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ ПОИСКОВЫМИ ДЕЙСТВИЯМИ В МОРЕ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

Поисковые действия имеют широкое распространение в различных областях деятельности как в мирное, так и в военное время. Эффективность поиска и обнаружения заданного объекта в значительной степени определяет успех не только боевых, но и гуманитарных, в том числе – спасательных операций. Разработка специального математического обеспечения управления поисковыми действиями представляет собой сложный и наукоемкий вид деятельности, связанный с необходимостью моделирования не только процессов поиска как таковых, но и сопутствующих им физических процессов – гидрометеорологических, распространения гидроакустических и радиолокационных сигналов и др. Вместе с тем, в рассматриваемой предметной области управления поисковыми действиями как теоретический аппарат, являющийся основой специального математического и программного обеспечения, так и расчетно-методические средства характеризуются наметившимся и все более нарастающим отставанием от требований практики и современного развития информационных технологий. Управление поисковыми действиями по прежнему сопровождается необходимостью выполнения ручных расчетов и графических построений по причине отсутствия аппарата автоматизированного планирования.

Целью проведенного автором исследования являлась разработка теоретического аппарата управления поисковыми действиями в море с использованием возможностей современных геоинформационных систем.

Для достижения указанной цели автором были решены следующие задачи:

- моделирование априорного распределения вероятности местоположения объекта поиска (если это необходимо – с учетом его движения до начала и в процессе поиска;
- определение закона (функции) обнаружения;
- определение поискового потенциала поисковой системы, в том числе определение эффективной дальности обнаружения поисковой единицы с учетом влияния факторов внешней среды на эффективность поиска;
- разработка плана поиска, в том числе решение задачи оптимального распределения поисковых ресурсов;
- определение оптимальных поисковых траекторий наблюдателей;
- оценка эффективности разработанного плана – определение вероятности обнаружения цели;

– корректура плана поиска в соответствии с достигнутыми в его ходе результатами, в том числе моделирование апостериорного распределения вероятности местоположения объекта поиска с учетом результатов проведенного поиска;

– решение задачи перераспределения поисковых ресурсов с учетом текущей поисковой ситуации;

– оценка эффективности поиска на предмет принятия дальнейших управленческих решений.

Для решения указанных задач использовались как фундаментальные научные методы, такие как метод байесовского оценивания, метод оценивания по критерию максимального правдоподобия, методы теории нечетких множеств, так и разработанные автором матричный метод моделирования распределений объекта поиска и метод оптимизации распределения поисковых ресурсов на основе энтропийного представления эффективности поиска.

Необходимо заметить, что эффективное решение указанных задач с учетом потребностей практики - прежде всего, с точки зрения оперативности принимаемых решений - в настоящее время немыслимо без использования возможностей современных геоинформационных систем.

В результате работы автором произведено усовершенствование существующих и создание новых методов и моделей теории поиска объектов, объединение и использование реализующих алгоритмов в единую структуру расчетных средств на основе современных геоинформационных технологий. Это позволило решить задачу их унификации; ситуативной гибкости (адаптивности) к условиям, целям и задачам поиска, составу и возможностям поисковых сил, а также географическим особенностям района поиска.

Смирнова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

О МЕТОДЕ ПРОГНОЗИРОВАНИЯ И ВИЗУАЛИЗАЦИИ ЗОН ВИДИМОСТИ РЛС С ИСПОЛЬЗОВАНИЕМ ГИС-ИНСТРУМЕНТОВ

Одной из наиболее сложных и актуальных задач в радиолокации является задача оперативного прогнозирования зон видимости радиолокационных систем (РЛС) в заданных гидрометеорологических условиях. Посредством моделирования можно заранее спрогнозировать предельные возможности РЛС по обнаружению различных объектов в заданной среде, в конкретных гидрометеорологических условиях. Получаемые сведения позволяют не только обеспечить высокую эффективность функционирования РЛС, но и оптимизировать ее работу, сэкономить материальные и энергетические ресурсы. С активным развитием геоинформационных технологий и систем мониторинга окружающей среды (в том числе космических) возможности более полного учета гидрометеорологических условий, таких как атмосферные осадки, волнение морской поверхности, становятся реальными. Однако это требует совершенствования самих математических методов оперативного построения зон видимости РЛС с учетом текущих гидрометеорологических условий.

Удобной платформой для решения поставленных выше задач служат геоинформационные системы. Они обеспечивают эффективную обработку огромных массивов информации, имеющих геопространственную привязку, а также оперативное наглядное представление полученных результатов на картографической подложке.

В состав ГИС входят также модули, обеспечивающие доступ к информации, связанной с текущими координатами объектов локации, самих РЛС. К такой информации также можно отнести все данные, касающиеся надводной и воздушной ситуации в районе действия РЛС. Данные модули являются основными источниками данных для решения радиолокационных задач.

В настоящее время разработан ряд достаточно строго обоснованных подходов к расчетам характеристик радиолокационной наблюдаемости и прогнозирования зон видимости РЛС в регулярной тропосфере, основанных на геометрооптическом приближении, учете дифракционных эффектов или методе нормальных волн. Однако эти методы не нашли широкого применения в прикладном прогнозировании зон видимости РЛС и вычислении характеристик радиолокационной наблюдаемости, что обусловлено сложностью расчетов для слоисто-неоднородной тропосферы. Также следует отметить, что отсутствуют результаты апробации этих методов на экспериментальных данных.

Предложенный метод оперативного прогнозирования зон видимости РЛС позволяет производить расчет характеристик радиолокационной наблюдаемости с учетом гидрометеорологических условий распространения электромагнитных волн (в условиях нерегулярной тропосферы). Численный метод решения основывается на пошаговом решении интегральных уравнений относящихся к классу уравнений Вольтерра с учетом наличия корневых особенностей на обоих концах промежутка интегрирования.

Предложенный метод был реализован в рамках математической библиотеке, входящей в состав комплекса радиолокационных расчетов характеристик радиолокационной наблюдаемости. Математическая библиотека позволяет существенно облегчить процесс моделирования зон видимости и вычисления характеристик радиолокационной наблюдаемости РЛС и содержит

специальный математический аппарат для решения этих задач. Также библиотека математических функций включает ряд функций специального вида (например, функции Эйри, Бесселя и т.д.).

Предложенный метод определения зон видимости РЛС с учетом гидрометеорологических параметров, позволяет: прогнозировать результаты радиолокационного наблюдения в заданном районе; адаптировать функционирование РЛС с учетом гидрометеорологической обстановки; определять характеристики электромагнитного поля в заданном районе функционирования РЛС с учетом аномальных условий распространения радиоволн; выбирать благоприятные маршруты движения воздушных и морских судов; выдвигать требования к техническим параметрам вновь проектируемых РЛС.

Предложенные решения могут быть использованы при обосновании способов применения РЛС и требований к ним.

Цветков М.В., Васильев П.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПЛАНИРОВАНИЕ ЭКОЛОГИЧЕСКИХ ПОИСКОВО-СПАСАТЕЛЬНЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОЙ ГЕОГРАФИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МОНИТОРИНГА МОРСКОЙ ОБСТАНОВКИ

В докладе оценивается возможность расширения функциональных возможностей интеллектуальной географической информационной системы мониторинга морской обстановки – основы для построения ситуационного центра информационного обеспечения экологических поисково-спасательных операций (ЭПСО), проводимых в Арктическом регионе РФ. Под интеллектуальной географической информационной системой (ИГИС) в статье понимается ГИС, которая включает в свой состав интегрированные средства и/или системы искусственной интеллектуальности.

Современный этап развития нефте- и газодобычи в Российской Федерации и ряде других стран непосредственно связан с разработкой шельфовых месторождений в Арктике. Освоение практически всех месторождений в шельфовой зоне Арктического региона сопряжено со значительными рисками возникновения чрезвычайных ситуаций различного масштаба.

Проведение экологических поисково-спасательных операций в Арктическом регионе РФ невозможно представить без качественной информационной и интеллектуальной поддержки управленческой деятельности всех задействованных в них организаций (министерств, ведомств, коммерческих предприятий). Следует отметить, что каждый из участников ЭПСО обладает не только собственным составом поисково-спасательных средств и технологий их применения, но и особыми представлениями о порядке и качестве их использования.

Одним из перспективных подходов к разрешению возможных разногласий является создание специального ситуационного центра поддержки принятия решений, позволяющего координировать совместные действия всех участников ЭПСО. По мнению авторов статьи информационная и интеллектуальная поддержка управленческой деятельности в таком ситуационном центре должна осуществляться с использованием технологии интеллектуальных географических информационных систем мониторинга морской обстановки и комплексного сценарного подхода.

В статье предлагается использовать общий сценарный подход к планированию и последующей оценке качества принятых оперативным штабом решений на проведение ЭПСО. В работе также разработаны методы интеграции информации от различных источников данных о ходе ЭПСО. В основе разработанных методов лежит понятие онтологии и единой модели информационного взаимодействия. Обработка входных данных производится на различных уровнях, что позволяет значительно снизить поток информации, поступающей в ситуационный центр.

Приводятся результаты использования предложенного сценарного подхода к планированию экологической поисково-спасательной операции в Арктическом регионе РФ.

Штрапов В.В.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь

О НЕКОТОРЫХ АСПЕКТАХ ИСПОЛЬЗОВАНИЯ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Повышение эффективности работы правоохранительных органов по раскрытию преступлений в настоящее время невозможно без интеграции в служебную деятельность новых информационных технологий. В настоящее время уже созданы и продолжают создаваться большое количество автоматизированных банков данных, содержащих самые разнообразные сведения. Речь идет о банках данных различных служб правоохранительных органов, налоговых и таможенных служб, регистрирующих органов, фонда социальной защиты, медицинских учреждений, банков и финансовых компаний, транспортных предприятий, авиа и железнодорожных касс, частных предприятий, оказывающих информационные услуги и т.д.

Соответственно, умение ориентироваться в таком объеме самых разнообразных сведений, представленных в электронном виде, освоение технологий доступа в нужные банки данных и получения требуемых сведений, разработка технологии их сопоставления представляет собой перспективное направление в решении правоохранительных задач.

В этой связи одним из направлений совершенствования процесса раскрытия преступлений является автоматизация процесса анализа больших объемов структурированной информации из различных источников путем ее графической визуализации на географических картах. Как предполагается, это позволит значительно сократить временные ресурсы на проведение информационно-аналитической работы, что позволит более оперативно решать оперативно-служебные задачи, своевременно реагировать на изменение складывающейся обстановки, и соответственно принимать своевременные управленческие решения, выявлять риски и угрозы в различных сферах.

В настоящее время имеется большое количество различных программных решений, позволяющих осуществлять географическую привязку определенных данных. Программы такой категории относят к так называемым географическим информационным системам (далее – ГИС).

В широком смысле ГИС – это система сбора, хранения, анализа и графической визуализации географических данных и связанной с ними информации о необходимых объектах. Понятие ГИС также используется в более узком смысле - как программного средства, позволяющего пользователям искать, анализировать и редактировать как цифровую карту местности, так и дополнительную информацию об объектах.

ГИС может включать в свой состав пространственные базы данных (в том числе, под управлением универсальных систем управления базами данных), редакторы растровой и векторной графики, различные средства пространственного анализа данных. Программные решения указанной категории в основном применяются в картографии, геологии, метеорологии, землеустройстве, экологии, региональном управлении, транспорте, экономике, обороне и многих других областях. Указанные программные средства используются для решения как научных, так и прикладных задач. Таковыми задачами могут быть учет и инвентаризация ресурсов (в том числе ведение кадастра), анализ, оценка, мониторинг, управление и планирование, поддержка принятия решений и т.п.

Указанные возможности ГИС могут быть использованы и для решения задач, стоящих перед правоохранительными органами. Причем, полагаем, что необходимо использовать не только графические возможности ГИС, как средство для пространственно-фактографического анализа, но и предполагается расширение функционала применения ГИС за счет наложения на определенную пространственную область формализованных данных, характеризующих состояние различных сфере, и имеющих значение для выполнения функций, стоящих перед подразделениями правоохранительных органов. К примеру, речь может идти сведениях о пунктах пропуска, количестве и характеристике товаров, перемещаемых через таможенную границу государства; данных об основных экономических показателях субъектов хозяйствования в масштабах региона и всего государства; о структуре населения, его занятости и уровне доходов; о наличии учреждений образования и культуры, туризма и отдыха; об инвестиционных показателях в привязке с экономическими результатами региона; о характеристике организаций по видам экономической деятельности, видам собственности и организационно-правовым формам; о показателях, характеризующих состояние и развитие промышленности, сельского хозяйства, торговли, транспорта, связи; о финансовой деятельности организаций, инвестициях, ценах и тарифах; об объемах внешней торговли товарами и услугами, структуре экспорта и импорта; о состоянии преступности и т.д.

Очевидно, что большинство из указанных сведений имеют открытый характер и могут быть использованы в процессе правоохранительной деятельности путем анализа данных получаемых из статистических и иных государственных органов, а также из средств массовой информации и сети Интернет (официальных сайтов государственных органов и организаций).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ РИСКОМ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Алексеев В. В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН

ЛВ-АНАЛИЗ НАДЕЖНОСТИ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ МЕТАЛЛУРГИЧЕСКОГО КОМБИНАТА

Рассматривается выбор предпочтительной схемы электроснабжения металлургического комбината с точки зрения надёжности. Изложен алгоритм решения задачи с помощью логико-вероятностного подхода. Разработаны структурная, логическая и вероятностные модели надёжности системы для трёх вариантов схемы подключения. Определены вклады элементов в надёжность.

Комбинат получает питание с районных подстанций мощностью 220 и 500 кВ (РПС-1 и РПС-2). Питание с районных подстанции поступает к технологическому оборудованию посредством трёх подстанций на территории комбината (ПС-1, ПС-2, ПС-3) через систему коммутационных подстанций. Вблизи располагается теплоэлектроцентраль (ТЭЦ-2), которая может работать в режиме источника электроснабжения или подстанции. От ТЭЦ-2 к системе подстанций протянута 21 кабельная линия.

Схема электроснабжения с учётом районных источников электроснабжения (ГРЭС-1 и ГРЭС-2) содержит длины воздушных и кабельных линий, которые учитывают при оценке надежности. Рассмотрен вопрос об исключении ТЭЦ-2 как источника энергоснабжения и переводе ее в режим котельной. Рассмотрена возможность сохранения ТЭЦ-2 в качестве подстанции. Сопоставлялись схем подключения комбината к внешним источникам:

Текущая схема подключения: РПС-1, РПС-2, ТЭЦ-2 (как источник и как подстанция).

Планируемая схема, вар.1: РПС-1, РПС-2, ТЭЦ-2 (как котельная и подстанция).

Планируемая схема, вар.2: РПС-1, РПС-2 (ТЭЦ-2 исключена).

Решаемая задача является характерной для систем с высоким уровнем резервирования, что приводит к повторным элементам и вычислительной сложности. Оценка и анализ надежности таких систем невозможны без применения программного комплекса типа Арбитр.

1. Построение структурной модели надёжности. Каждому элементу, для которого учитывают надежность, поставлена в соответствие вершина, имеющая свой идентификатор. Вершины соединяют направленными дугами. Квадратами обозначены воздушные и кабельные линии электропередач, кругами – источники электроснабжения, шестиугольниками – подстанции.

2. Построение Л-модели надёжности. Каждой вершине структурной модели поставлена в соответствие Л-переменную. Она может принимать значения: 0 – если элемент неисправен и 1 – если он исправен. По схеме установлены кратчайшие пути успешного функционирования (КПУФ). Их число равно 15. Их описывают 21 инициирующее событие. Функция успешного функционирования системы представлена в ДНФ.

3. Построение В-модели надёжности. Л-модель системы в форме КПУФ нельзя использовать для расчетов надежности из-за повторных элементов. Программный комплекс «Арбитр» перевел Л-модель к ортогональной форме, в которой вместо Л-переменных подставляют их вероятности и получают В-модель надежности, которая содержит 171 слагаемое, каждое из которых есть произведение до 16 сомножителей..

Надежность системы оценивалась на В-модели. При исключения элемента (источника питания, подстанции или линии электропередачи), вероятность его успешного функционирования задают 0. Вероятности отказов элементов системы рассчитаны по числу отказов в год. Для воздушных и кабельных линий число отказов заданы по статистике, для источников электроэнергии\подстанций вероятности определены экспертно.

4. Исследования. С помощью обнуления вероятности успешного функционирования для ряда вершин получены следующие результаты для трёх схем подключения. Под отказом подразумевается полное отключение электроэнергии с последующим разрушением основного технологического оборудования.

Голоскоков К.П., Чиркова М.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРОБЛЕМА ПРОЕКТИРОВАНИЯ СИСТЕМЫ КОРПОРАТИВНОЙ БАЗЫ ЗНАНИЙ

В современном мире информация и знания становятся источником конкурентного преимущества. Международная исследовательская компания KMPG опубликовала данные,

свидетельствующие о возрастающем интересе к управлению интеллектуальным капиталом компании: 81% ведущих европейских и американских организаций применяют техники управления знаниями. В связи с этим проблема управления знаниями в организации выходит на первые планы. Решением данной проблемы может стать переход на работу с корпоративной базой знаний в компании. Однако внедрение корпоративной базы знаний – это процесс дорогостоящий и требует больших трудозатрат, поэтому прежде, чем приступить, необходимо определить подходящую для компании структуру базы. База знаний должна быть встроена в контекст организации, для того чтобы сотрудники постоянно использовали базу знаний в своей профессиональной деятельности, необходимо создать простую для понимания персоналом структуру хранения данных, которая будет соответствовать деятельности организации. Исходя из этого, проблема выбора оптимальной структуры базы знаний является основополагающей при проектировании. База знаний может повысить эффективность совместной работы в коллективе, а также позволит сократить время на адаптацию новых сотрудников. Особенно важным этот инструмент может стать для территориально распределенных предприятий или сетевых организаций. Наличие корпоративной базы знаний позволяет компаниям решать множество важных вопросов. К ним относится сокращение времени поиска информации. Согласно исследованиям IDC, в среднем работники тратят от 15% до 35% рабочего времени на поиск необходимой информации для решения профессиональных задач, при этом 40% таких сотрудников не находят искомого. Кроме того, в процессе поиска требуемой информации сотрудники отвлекают от работы своих коллег, что также наносит урон эффективной работе компании. Хорошо организованная база знаний поможет компании сократить расходы, уменьшив время поиска требуемой информации. Корпоративные базы знаний разрабатываются под потребности каждого отдельного предприятия, поэтому единой структуры организации баз нет. Для того чтобы разобраться, какие классификации разделов используются компаниями, проанализируем имеющиеся базы знаний, данные о которых находятся в открытом доступе. Бенчмаркетинговая компания TheAmericanProductivity&QualityCenter (APQC) предложила следующую классификацию процессных фреймворков базы знаний:

1. разработка стратегии и видения;
2. разработка и управление продуктом или услугой;
3. изучение рынков, продажи продуктов и услуг;
4. управление обслуживанием клиентов;
5. разработка и управление человеческим капиталом компании;
6. управление информационными технологиями;
7. управлениефинансовыми ресурсами;
8. приобретение, выстраивание структуры и управление активами компании;
9. управление рисками;
10. управление внешними взаимоотношениями;
11. разработка и управление бизнес-возможностями. ИТ-компания «+Альянс», которая предоставляет комплексные услуги по разработке и управлению ИТ-инфраструктурой, реализовала в своей базе знаний структуру разделов на основе часто решаемых внутри компании проблем.

Компания PRIZMXXVII, занимающаяся разработкой и продвижением сайтов, создала базу знаний на основе деления по видам продуктов и технологий, представляемых компанией. Другая российская ИТ-компания разработала базу знаний на основе типов хранимой в ней информации: инструкции, статьи, ссылки, утилиты.

Компания «Богданов и партнеры», предоставляющая клиентам услуги по повышению эффективности бизнеса за основу своей базы знаний взяли классификацию по проектам, в рамках которых выделили следующие разделы: справочник рисков; журнал извлеченных по проекту уроков; библиотека типовых фрагментов; кейсы по управлению проектом; публикации; данные о клиентах; шаблоны проектных документов.

Компания ПитерСофт, специализирующаяся на автоматизации бизнеса в своей базе знаний по управлению процессами выделила следующие разделы: глоссарий, содержащий термины, используемые в системе; часто задаваемые вопросы, возникающие при работе с системой; решения типовых задач бизнеса; примеры бизнес-процессов.

Таким образом, можно выделить следующие типы классификаций структуры баз знаний:

- по видам продуктов и услуг, предоставляемых компанией;
- по организационнойструктуре;
- по областям деятельности компании;
- по классификации решаемых в компании проблем;
- по проектам компании;
- по типу документов, хранящихся в базе.

Автор предлагает классифицировать разделы баз знаний на основе структурных подсистем организации. В основе данной классификации лежит метод структурного анализа предприятия.

Ежгуров В.Н., Доброрадова В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ПРЕДЛОЖЕНИЕ ПО РЕАЛИЗАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖАНИЯ И СОПРОВОЖДЕНИЯ ПРОЕКТОВ

В настоящее время множество крупных организаций, чья деятельность осуществляется как взаимодействием разрозненных, так и единых рабочих коллективов. Такие коллективы могут находиться как на одной площадке, так и на множестве разрозненных. Их деятельность связана с реализацией огромного числа проектов, как внешних, так и внутренних. Для того чтобы организовывать деятельность таких коллективов, отслеживать этапы выполнения проектов и упрощения подготовки документации целесообразно создать автоматизированную систему для формирования проекта. Такая система позволит формировать проект на основании данных, поступающих как от других автоматизированных систем организации, так и от персонала, задействованного в реализации проектов.

Из-за большого размера организации следует дополнительно добавить для системы:

- работа с большим числом пользователей;
- возможность разграничения доступа к системе в зависимости от роли пользователей.

Годовая комплексная программа закупок состоит из следующих разделов:

- техническое перевооружение и реконструкция – совокупность лотов по техническому перевооружению, реконструкции и модернизации;
- ремонты – совокупность лотов по ремонту;
- научно-исследовательские разработки – совокупность лотов по испытаниям, опытам и исследованиям;
- техническое обслуживание – совокупность лотов по техническому обслуживанию.

Годовая комплексная программа закупок подразделяется на плановую и внеплановую.

Формирование проекта годовой комплексной программы закупок должно происходить на основе конкретных версий титулов. Дополнительно необходимо предусмотреть оповещения по любым изменениям работ, включенным в лоты. На усмотрение пользователя должна быть возможность настраивать оповещения.

В системе должна быть предусмотрена возможность пересчета лотов по любой утвержденной версии производственной программы, а также рабочей версии. При пересчете параметров годовой комплексной программы закупок должна быть возможность зафиксировать версию конкретного лота, при этом остальные лоты должны пересчитываться по выбранной версии производственной программы.

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет

ПРЕДЛОЖЕНИЯ ПО ВНЕДРЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПЛАНИРОВАНИЯ ПРОИЗВОДСТВЕННЫХ ПРОГРАММ

Бизнес-процессы крупных организаций настолько сложны, что зачастую требуется внедрение автоматизированной системы планирования производственных программ (ПП), предназначенных для управления деятельностью по формированию, согласованию и исполнению среднесрочных и долгосрочных производственных программ организации.

На такие системы накладывается ряд требований, связанных с размерами организации, к примеру, уровень образования сотрудников, их количество, зачастую более 100 пользователей; реализация механизма разграничения прав доступа пользователей в виду сложной иерархии таких организаций; реализация интегрированной системы информирования пользователей о событиях на основе настраиваемого календаря и многое другое, что будет использоваться организацией.

При разработке таких автоматизированных систем следует учитывать, что могут быть выделены несколько видов производственных программ, например:

- программа технического перевооружения и реконструкции (ТПиР) – совокупность инвестиционных проектов по техническому перевооружению, реконструкции и модернизации, включающих в себя необходимые для их реализации мероприятия (работы и услуги);
- программа ремонтов – совокупность работ по ремонту;
- программа научно-исследовательских разработок (НИР) – совокупность работ/услуг по испытаниям, опытам и исследованиям.
- программа технического обслуживания (ТО) – совокупность мероприятий по техническому обслуживанию.

А также планирование можно делить на:

- долгосрочную ПП организации – это долгосрочные ПП ТПиР организации на плановый период 15 лет и более. Долгосрочная ПП организации является основным инструментом реализации

стратегии. Процесс формирования долгосрочной ПП организации осуществляется 1 раз в пять лет (при необходимости корректируется 1 раз в 2 года).

– среднесрочную ПП организации – ПП, формирующаяся на основании долгосрочной ПП, актуальной среднесрочной ПП, состоящая из набора конкретных инвестиционных проектов (а также мероприятий, входящих в их состав) с учетом фактического исполнения ПП за прошедший период. Среднесрочная ПП формируется на 6 лет и пересматривается ежегодно с добавлением нового годового горизонта, при этом содержит все мероприятия вне зависимости от срока их реализации, необходимые для реализации инвестиционных проектов, вошедших в состав ПП.

В системе должен быть реализован функционал ведения и актуализации реестра (базы) инвестиционных проектов ТПиР.

В части признаков (критериев) необходимо предусмотреть:

– возможность проставления процентов от затрат и суммы затрат на работу, который приходится на каждый признак, а также экономического эффекта от работ;

– возможность включения и отключения контроля непревышения суммы всех затрат по признакам над бюджетом работы.

В Системе необходимо предусмотреть возможность просмотра и сравнения между собой любых версий ПП.

Система должна иметь обратную связь с контуром исполнения производственных программ ремонтов, ТО, НИР, ТПиР.

В связи с планированием ПП на несколько лет вперед необходимо предусмотреть индексацию ПП в соответствии с проставленными условиями индексациями и выбранными едиными сценарными условиями.

В Системе должен быть предусмотрен механизм параллельного планирования среднесрочной и долгосрочной ПП. При этом должны быть реализованы правила автоматического применения изменений, связанных изменений с проверками.

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет

ПРЕДЛОЖЕНИЯ ПО РАСШИРЕНИЮ В АВТОМАТИЗИРОВАННУЮ СИСТЕМУ УПРАВЛЕНИЯ ПРОЕКТАМИ ПОДСИСТЕМУ ОПТИМИЗАЦИИ ПРОЕКТОВ

В современном обществе крупные организации используют автоматизированные системы, призванные повысить производительность выполняемых работ. Для этих целей создаются по архитектуре системы, которые «ведут» проекты на всех этапах жизненного цикла. Зачастую уровень выполнения основных функций таких программ настолько высок, что изменения внешней среды – условий реализации проекта мгновенно обрабатываются, и негативный эффект сглаживается.

Компоненты автоматизированной системы, выполняющие данные функции, могут называться по-разному, но все они предназначены для:

– формирования сценариев технических воздействий с учетом вероятности отказа оборудования, уровня рисков отказа, загрузки персонала подрядчика;

– обеспечения технико-экономического анализа сценариев технических воздействий.

На эти компоненты также действуют те же требования, как и на всю систему в целом, к примеру:

– работа с большим количеством пользователей одновременно;

– информирование о важных для проектов событиях;

– разграниченный доступ.

Возможные сценарии должны носить рекомендательный характер при планировании производственной программы (ПП), т.е. пользователь должен иметь возможность выбрать один из сценариев и применить в ПП на свое усмотрение.

Сценарии реализации ПП (предполагаемые сроки и объемы реализации технических воздействий) формируются с учетом внешних режимных, финансовых и ресурсных ограничений.

Технико-экономический анализ сценариев технических воздействий основывается на результатах:

– оценки технического состояния оборудования;

– прогнозирования вероятности наступления отказа оборудования;

– оценки уровня рисков отказа оборудования;

– уровня загрузки, квалификации и территориального распределения персонала подрядчика.

В общем случае технико-экономический анализ сценариев технического перевооружения и реконструкции объектов проектной работы должен быть основан на следующих экономических категориях:

– эксплуатационные расходы на оборудование (ремонты и техническое обслуживание, затраты на собственные нужды и т.д.);

- уровень потенциальных рисков отказа оборудования;
- накладные расходы (фонд оплаты труда, амортизация и т.д.);
- налоговые отчисления (налог на имущество, водный налог и т.д.)
- доходы от основной деятельности (производство электроэнергии, предоставление мощности).

Карасев В.В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН

ОЦЕНКА РИСКА ИНФРАСТРУКТУРЫ ЛОГИКО-ВЕРОЯТНОСТНЫМ МЕТОДОМ

Управление инфраструктурой – это процесс, который содержит в себе технический аспект (ремонт и эксплуатация) и экономический аспект (распределение инвестиций). Есть инфраструктура, финансируемая государством - социальная инфраструктура, объекты оборонного значения; есть инфраструктура, финансируемая коммерческими структурами - частные заводы и предприятия; и существует инфраструктура, инвестируемая совместно государством и бизнесом на условиях равноправного партнерства.

Чтобы эффективно управлять инфраструктурой и рационально распределять инвестиции, необходимо знать ее «слабые» звенья и принимать меры к их «усилению». Показателем «слабости» отдельного объекта инфраструктуры может выступать его риск – вероятность отказа. Оценка риска позволит спрогнозировать развитие ситуации (изменение состояния инфраструктуры) и выявить те объекты, которые острее всего нуждаются в инвестициях.

Задача может быть решена достаточно просто с использованием математического аппарата исчисления предикатов и логико-вероятностного моделирования.

Каждый объект i инфраструктуры R описывается n-арным предикатом Vi = {m1, m2, ..., mn}, где параметры mj, j = 1, ..., n - аргументы предиката, описывающие состояние объекта, от которых зависит его работоспособность, например, m1 — величина остаточного ресурса объекта в целом (часто измеряется временем, прошедшим с момента капитального ремонта), m2 — уровень обеспеченности запасными частями, m3 - степень износа критически важных узлов, m4 — уровень контроля состояния инженерных систем, m5 - целостность функциональных связей с другими объектами, и т.д. Если значения аргументов не превышают некоторых допустимых пороговых (критических) значений, то Vi = {m1, m2, ..., mn} = 0, т.е. объект работоспособен, в противном случае Vi = {m1, m2, ..., mn} = 1, объект неработоспособен.

Предикат по сути - это высказывание, содержащее неопределенность, и о нем невозможно судить, является он истинным или ложным. Поэтому для каждого объекта инфраструктуры имеется еще один параметр - вероятность того, что при заданном наборе параметров {m1, m2, ..., mn} объект станет неработоспособным, т.е. соответствующий объекту предикат примет значение P(Vi = 1). Отказ объекта является случайным событием, вероятность которого зависит только от параметров самого объекта и внешних случайных событий. Отказы объектов инфраструктуры в совокупности являются независимыми случайными событиями, так как выход из строя объекта (событие) не зависит от параметров тех объектов, которые связаны с ним функциональными связями.

Строятся логическая и вероятностная функции риска инфраструктуры и по ним вычисляются риски объектов. После вычисления рисков мы можем провести анализ вкладов объектов в интегрированный риск инфраструктуры. Интегрированный риск P(R = 1) показывает, насколько вероятен коллапс всей инфраструктуры. Эта величина может быть получена путем логического сложения рисков критичных объектов и используется для задач анализа. В инфраструктуре есть критические объекты, отказ которых влечет за собой отказ всей инфраструктуры, и объекты второстепенные, отказ которых приведет к проблемам у потребителей, но не к коллапсу инфраструктуры. Если ввести в логическую функцию логические переменные, отвечающие за состояние второстепенных объектов, то она значительно усложнится.

Вычисляя вклады рисков объектов в интегрированный риск инфраструктуры и упорядочивая объекты по возрастанию вкладов, мы получаем ответ на вопрос о распределении инвестиций. Решение о распределении инвестиций производится по значениям рисков объектов, их вкладам в интегрированный риск инфраструктуры и степени критичности.

Предлагаемый метод прост в использовании, универсален, требует минимум исходных данных (при этом в зависимости от наличия данных возможна разномасштабная детализация объекта), обеспечивает прозрачные результаты и приемлемую точность. Повышение точности требует оперативного обновления информации о состоянии объектов (степени износа основных элементов,) и внешней среды (прогнозирование паводков, штормов, землетрясений).

Метод пригоден для коммерческих структур (владеющих объектами и средствами производства с разветвленной инфраструктурой), аналитических отделов государственных органов экономического развития (для прогнозирования аварий и отказов объектов инфраструктуры и распределения инвестиций с целью предотвращения отказов), ситуационных центров (для системы мониторинга и оперативного прогнозирования развития текущей ситуации, изменения состояния сложной системы).

Метод является фундаментальным и позволяет анализировать надежность и безопасность самых разных типов инфраструктур различного назначения: социальной, транспортной, инженерной, экономической, информационной, военной, рыночной, инновационной.

Карасева Е.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

МЕТОДИКИ ОЦЕНКИ НАДЕЖНОСТИ БАНКА

Комплексная оценка надежности банка, необходима, чтобы сократить убытки населения и предприятий. При неэффективной оценке финансового состояния кредитной организации может обернуться недоверием вкладчиков и оттоком денежных средств, а также повышения платы АСВ.

Рассмотрим методики, применяющий комплексный показатель надежности, которые применяются на практике. Методика оценки финансового состояния кредитной организации, предложенная ЦБ РФ, регулируется Указанием Банка России от 31.03.2000 №766-У (ред. от 21.12.2000) «О критериях определения финансового состояния кредитной организации», а также Указанием от 30 апреля 2008 г. №2005-У «Об оценке экономического положения банков».

В первую очередь осуществляется анализ четырех групп показателей: активов, капитала, доходности и ликвидности. После расчета всех коэффициентов каждого блока осуществляется расчет обобщающего результата по группам показателей оценки капитала (РГК), активов (РГА), доходности (РГД) и ликвидности (РГЛ). Рассматриваемый обобщающий показатель определяется как средневзвешенное значение всех рассчитанных величин каждого блока.

Кроме того, Банк России определяет 9 нормативов, обязательных для расчета и соблюдения каждой кредитной организацией. Рассмотрим подробнее каждый из них. Нормативы устанавливаются Банком России, а порядок их расчета регламентируется Инструкцией от 3 декабря 2012 года №139-И «Об обязательных нормативах банков». Чаще всего именно нарушение этих нормативов служит для отзыва лицензии банка.

Методика Агентство страхования вкладов. Еще одним подходом к оценке надежности банка является подход, сформулированный Банком России в Указании от 16.01.2004 №1379-У «Об оценке финансовой устойчивости банка в целях признания ее достаточной для участия в системе страхования вкладов».

Если банк входит в систему по страхованию вкладов (ССВ), то в случае наступления страхового случая (отзыв лицензии на осуществление банковских операций), его вкладчику выплачивается денежная компенсация — возмещение по вкладам в размере до 1,4 млн рублей. В случае ликвидации банка (признания его банкротом) его расчеты с вкладчиком в части, превышающей указанную выплату, проводятся позднее, в ходе ликвидационных процедур (конкурсного производства) в банке (при наличии у банка средств).

Для анализа финансовой устойчивости кредитной организации в соответствии с Указанием №1379-У используется балльная методика, оценивающая 5 групп показателей:

- показатели оценки капитала;
- показатели оценки активов;
- показатели оценки доходности;
- показатели оценки ликвидности;
- показатели оценки качества управления банком, его операциями и рисками

Методика оценивания на основе рейтинговых агентств. Это наиболее близкая методика, которая учитывает интегральный показатель надежности кредитного учреждения. Однако, получения рейтинга международных агентств стоит денег и его необходимо каждый год подтверждать(тоже за определенную плату). В российских реалиях это сводится к тому, что только крупные и системнозначимые банки могут позволить данную процедуру, мелким и даже средним – она не по карману. В настоящее время в стране существуют и национальные рейтинговые агентства. Однако, любой прогноз субъективен и быстро может измениться положения банка. Все представленные рейтинги для банков строятся лишь по одному показателю – кредитные рейтинги. Кредитные рейтинги представляют собой мнения российских и зарубежных рейтинговых агентств о кредитоспособности и финансовой устойчивости банков РФ, как в рамках страны, так и в международных масштабах.

В работе предлагается использовать логико-вероятностный (ЛВ) метод. Выбор метода ЛВ-моделирования, обусловлен широким применением для оценки надежности в сложных технических системах и успешным применением в экономических системах для оценки вероятности операционного, кредитного рисков и риска портфеля ценных бумаг банках. Этот метод основан на построении сценария риска как дерева событий, соединенных логическими связями И, ИЛИ, НЕ, что позволяет построить логические и вероятностные модели для оценки и анализа рисков. Предлагаем развитие метода и применение его для оценки, уровня надежности банка. Преимуществом данного метода является возможность построения комплексной интегрированной модели риска. Подобная

задача ранее не решалась. Для оценки вероятностей инициирующих событий планируется адаптировать и использовать методы идентификации ЛВ-моделей по статистическим данным, использовать частотный анализ.

Карасев В.В., Карасева Е.И.
Россия, Санкт-Петербург, Институт проблем машиноведения, Санкт-Петербургский государственный университет аэрокосмического приборостроения

УПРАВЛЕНИЕ БАНКОМ ПО КРИТЕРИЮ ИНТЕГРИРОВАННОГО РИСКА

Экономическая безопасность государства обеспечивается стабильной экономикой. Стабильность экономики обеспечивается надежностью ведущих предприятий (крупнейших налогоплательщиков) и банковской системы. При этом банковская система играет ключевую роль в экономической безопасности государства, так как банки контролируют все денежные потоки.

В современных российских банках развиваются в первую очередь те системы и направления, которые дают быструю экономическую отдачу - реклама, рисковые финансовые операции, расширение перечня предоставляемых услуг, поиск новых рынков. И существенно отстают области системного анализа, диагностики, прогнозирования внешней и внутренней среды банка, разработки гибких стратегий, создания адаптивных структур.

Управление современными банками производится по критерию прибыли. Решения и управляющие воздействия направлены на максимизацию прибыли, что всегда влечет увеличение риска дефолта банка. В результате банковская система перестает быть надежной, так как возрастает число банков с высоким риском. Частые отзывы лицензий у банков подтверждают это.

Банк представляет собой сложную систему, надежность которой определяют не только финансово-экономические показатели, но и надежность технических средств и информационных систем. Не стоит забывать и о человеческом факторе.

Мы предлагаем разработать технологию оптимального управления банком по критерию интегрированного риска. Под интегрированным риском понимается вероятность дефолта (разорения) банка. Мы вводим показатель эффективности банка как отношение прибыли к риску. Управление по критерию риска подразумевает принятие решений и управляющих воздействий, направленных на уменьшение величины риска и увеличение его прибыли, т.е. на увеличение эффективности. Величина интегрированного риска может использоваться как рейтинг надежности банка, а совокупность этих величин по всем банкам может использоваться для оценки и анализа надежности всей банковской системы. Объект управления – это банк. Критерий управления — величина интегрированного риска. Критерий качества управления - величина эффективности банка. Чем выше эффективность, тем выше качество управления. Цель управления – повышение эффективности банка, определяемой как отношение прибыли к риску. Банк работает в условиях непредсказуемой и нелинейной экономической среды, которую определяет множество объективных и субъективных факторов. В этих условиях задача оптимального управления является некорректно поставленной задачей (ее решение не зависит от исходных данных), поэтому ее нужно решать специальными численными методами.

Для решения задачи используется комбинация нескольких научных подходов - методы системного анализа, теория оптимального управления и нечетких множеств (для принятия решений), логико-вероятностный метод (для расчета и анализа банковских рисков), методы структурной композиции/декомпозиции (для разработки моделей интегрированного риска), методы машинного обучения (переход от базы данных к базе знаний, идентификация логико-вероятностных моделей по статистическим данным и по нечисловой, неточной и неполной экспертной информации).

Технология может быть внедрена как аналитический инструмент в составе экспертных систем банков (для оптимального управления банком), инвестиционных компаний, Федеральной Службы Финансового Мониторинга, Счетной Палаты и Центробанка (для оценки и динамического анализа состояния банковской системы, заблаговременного выявления «проблемных» банков и оценки вероятности нежелательных событий). Внедрение технологии повысит надежность банковской системы РФ вследствие своевременного выявления «слабых» звеньев системы и принятия соответствующих превентивных мер. Внедрение технологии приведет к усилению и стабильности банковской системы, сократит количество отзывов лицензий. Модель риска банковской системы может быть использована регуляторами в составе экспертных систем для оценки, анализа и управления безопасностью всей банковской системы в целях повышения экономической безопасности государства. Технология позволит сократить экономические потери субъектов экономики, повысит надежность банковской системы и уровень экономической безопасности государства. Впервые появится эффективный инструмент для динамического управления экономической безопасностью путем вычисления вкладов инициирующих событий в риск отдельных банков и всей банковской системы и принятии соответствующих мер.

Вследствие своей универсальности технология может послужить в перспективе основой для систем искусственного интеллекта управления экономической безопасностью.

Соложенцев Е. Д.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ»

В дисциплине введены новые типы булевых «событий-высказываний» в экономике: о неуспехе объектов и субъектов, о невалидности, концептуальные события-высказывания, индикативные события-высказывания, события-высказывания о латентности, несовместные события-высказывания и др. и новые типы логико-вероятностных (ЛВ) моделей риска в экономике: гибридные ЛВ-модели неуспеха в управлении социально-экономическими системами, ЛВ-модели невалидности, концептуальные ЛВ-модели прогнозирования, индикативные ЛВ-модели опасности.

Объекты исследования топ-экономики — социально-экономические системы: СЭС-1 — наивысшей важности для государства, предназначенные для уменьшения потерь средств и увеличения их поступления; СЭС-2 — комплексные, зависящие от нескольких министерств и ведомств; СЭС-3 — локальные для предприятий. Рассмотрены задачи топ-экономики: построение ЛВ-моделей; ЛВ-анализ; ЛВ-прогнозирование и ЛВ-управление риском СЭС. Решаются задачи моделирования риска, анализа и управления риском Список предметного указателя дисциплины содержит 26 разделов, в которых названы 145 указателя (в скобках указано число указателей):

1. Анализ риска в социально-экономических системах (6);
2. Булевы события-высказывания в управлении экономикой (8);
3. Динамичность ЛВ-моделей риска (5);
4. Достоинства и особенности топ-экономики (12);
5. Классы ЛВ-моделей риска (5);
6. Компоненты топ-экономики (7);
7. Модели топ-экономики (4);
8. Мониторинг и управление процессом кредитования банка (4);
9. Невалидность (4);
10. `Объекты в топ-экономике (3);
11. Операционный риск банка и резервирования капитала по Базель (3);
12. Примеры СЭС приложений топ-экономики (10);
13. Противодействие взяткам и коррупции (4);
14. Противодействия наркотизации страны (3);
15. Процедуры технологии для классов (6);
16. СЭС-1 наивысшей важности для страны (6);
17. Свойства топ-экономики (12);
18. Синтез вероятностей событий для ЛВ-моделей риска (3);
19. Специальные Software (10);
20. Состояние топ-экономики (6);
21, Технологии управления риском (4);
22. Топ-экономика (3);
23. Управление качеством систем по ВТО (2);
24. Управление риском в СЭС (4);
25. Управление риском системы инноваций страны (4);
26. Управление риском экономического состояния России (5).

Начальный фрагмент Index научной дисциплины приведен ниже:

Анализ риска в социально-экономических системах:

- вклады в левом и правом “хвостах” распределения,
- вклады событий на плюс и на минус,
- экономические войны с санкциями,
- опасные события и их комбинации,
- структурная и вероятностная значимость событий,
- частотный анализ событий.

Булевы события-высказывания в управлении экономикой:

- индикативные события,
- концептуальные события,
- латентные события,
- невалидные события,
- несовместные события,
- сигнальные события,
- события неуспеха объектов,
- события неуспеха субъектов.

Соложенцев Е. Д., Карасев В.В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН

БАЗЫ ДАННЫХ И УПРАВЛЕНИЕ РИСКОМ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТЬЮ СИСТЕМ

Рассматривается один из разделов нового научного направления в экономической науке. Авторы руководствовались, в основном, идеями Дж. Буля по логике оценки истинности высказываний и лауреатов Нобелевской премии Джеймса Бьюкенена и Джеймса Хекмана о связи экономики и политики в развитии государства на основе теории игр и анализа статистических данных.

В развитие этих работ предложен новый подход к анализу и управлению экономической безопасностью социально-экономических систем (СЭС) на основе топ-экономики, использующей ЛВ-исчисление и понятия невалидности событий и систем. Рассматриваются связи экономики, государства, политики, бизнеса, науки и общества. В ЛВ-модели риска учитываются: инициирующие события, зависящие от государства, бизнеса, науки и общества, а также сигнальные события об изменениях в экономике, политике, праве, инновациях и ситуации на мировом рынке.

Невалидность системы – это отклонение ее состояния от значения, заданного техническим заданием и техническими условиями. Невалидность показателя системы – это отклонение его значения от заданного или нормативного.

Топ-экономика имеет унифицированную систему моделей, методов, технологий и специальные Software для управления социально-экономической безопасностью СЭС. Для обозначения этой унифицированной системы знаний и методов, базой которых служат ЛВ-модели риска и ЛВ-исчисление, предлагается название «топ-экономика».

Формулируется и исследуется проблема использования БД для логико-вероятностного управления риском и эффективностью систем. Излагается методика преобразования любой табличной базы данных в табличную базу знаний и систему логических уравнений. Приводятся примеры преобразования характерных БД в БЗ и построения логико-вероятностных моделей: кредитного риска банка, риска портфеля ценных бумаг, риска и эффективности ресторана. Решаются новые задачи. Рассмотрено управление безопасностью системы по одному состоянию по индикативной ЛВ-модели невалидности. Описаны разработанные специальные Software.

В настоящее время накопление информации для управления в системах производят в базах данных, которые используются для построения графиков, регрессий и т.д. Решаются задачи: классификация объектов с использованием средств машинного обучения Machine Learning.

В работе решается проблема использования БД для построения логико-вероятностных (ЛВ) моделей риска для решения задач оценки, анализа и управления риском и эффективностью систем. Для этого БД преобразуются в БЗ и, далее, строятся ЛВ-модели риска и решаются задачи анализа и управления риском и эффективностью систем с использованием специальных Software.

Цель работы – Сформулировать и исследовать проблему использования БД для логико-вероятностного управления риском и эффективностью систем.

Задачи работы: изложить методику преобразования БД в БЗ для ЛВ-управления риском и безопасностью систем; изложить методики ЛВ-управления по характерным БД: кредитный риск банка, портфель ценных бумаг, риск и эффективность ресторана; описать построение индикативной ЛВ-модели опасности (невалидности) по одному состоянию системы; описать разработанные специальные Software для ЛВ-управления риском и эффективностью систем по БД.

Характерные БД отличаются тем, что в одних (например, кредитный риск банка) эффективность состояний (кредитов) известно (хороший / плохой); в других (например, портфель активов) эффективность состояний (доходность портфеля) вычисляется; в третьих (например, товарооборот ресторана или прибыль предприятия) эффективность состояний известна. Соответственно, по разному формулируются и цели управления.

Основные результаты работы следующие:

1. Сформулирована проблема использования БД для логико-вероятностного управления риском и эффективностью систем, заключающаяся в преобразовании табличной базы данных в табличную базу знаний, записи системы логических уравнений и ЛВ-модели риска, анализе и управлении риском системы.

2. Изложена методика преобразования БД в БЗ на основе введения событий--градаций для параметров состояния системы, событий появления и событий неуспеха состояний системы, групп несовместных событий.

3. Изложены характерные примеры построения и использования ЛВ-моделей риска по базам данных: кредитный риск банка, риск портфеля активов, риск и эффективности ресторана.

4. Описана методика построения индикативной ЛВ-модели опасности (невалидности) по одному состоянию системы.

5. Описаны специальные Software для ЛВ-управления риском и эффективностью систем.

Крюкова Е.А., Козлова В.И. , Соложенцев Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

GlOBAL INNOVATIVE INDEX И КОМПЛЕКС ЛВ-МОДЕЛЕЙ ДЛЯ УПРАВЛЕНИЯ СИСТЕМАМИ ИННОВАЦИЙ

Выполнен анализ состояния и развития проблемы оценки инновационного индекса стран. Изложена методики оценки Глобального Инновационного Индекса (GII) и установлены ее недостатки для анализа и управления системами инноваций. Разработан комплекс логико-вероятностных (ЛВ) моделей для анализа и управления системами инноваций стран, включающий в себя модель ЛВ-модель глобального инновационного индекса (LP GII), гибридную ЛВ-модель риска неуспеха системы инноваций и индикативную ЛВ-модель опасности системы инноваций. Выполнена сравнительная оценка GII и LP GII рейтингов систем инноваций России, Финляндии, Швейцарии, США и Китая и др.

По рейтингу качества система инноваций Россия стоит на 62 месте из 142 стран мира. Поэтому актуальны научные исследования и разработки по повышению качества системы инноваций страны. Для управления социально-экономическими системами (СЭС) необходимы ресурсы. Поэтому актуальны проблема разработка моделей для управления инновациями с целью снижения потерь средств и увеличения их поступления от промышленности и бизнеса.

Работы лауреатов Нобелевские премии Д. Бьюкенена и Д. Хекмана рассматривают связи экономики и политики в развитии государства на основе теории игр и анализа статистических данных. В развитие этих работ в России разработан новый подход к анализу и управлению социально-экономической безопасностью систем на основе «Топ-экономики». Связи экономики, политики, науки и общества рассматриваются в широком аспекте. При разработке ЛВ-моделей риска использованы основные понятия топ-экономики: невалидность системы, новые булевы события-высказывания и новые типы ЛВ-моделей риска. Расчеты выполнены на Software Arbiter and Expa,

Цель работы: разработка комплекса ЛВ-моделей для оценки, анализа и управления системами нноваций стран, регионов, предприятий.

Анализ проблемы оценки инновационного индекса стран выполнен по отчету «Глобальный инновационный индекс 2013», который является результатом сотрудничества между Корнелльским университетом (Cornell University), бизнес-школой INSEAD и Всемирной организацией интеллектуальной собственности (WIPO).

Инновационный индекс GII, индексы IIP, IIR, производные показатели первого и второго уровней и 84 исходных показателя определяют состояние и привлекательность системы инноваций страны. GII позволяет сравнивать качество систем инноваций стран по их рейтингам. Однако, GII не позволяет анализировать и управлять системой инноваций страны. GII и другие производные индексы вычисляются арифметическим сложением с усреднением исходных показателей. Поэтому не позволяют определить влияние каждого исходного показателя на GII, производные показатели.

Основными результатами настоящей работы являются:

1. Выполнен анализ состояния и развития проблемы оценки глобального инновационного индекса стран. Проблема GII имеет большую практическую значимость. Однако GII не решает вопросы анализа и управления системами инноваций.
2. Выполнен анализ методики «Оценка GII стран» и установлены ее недостатки для анализа и управления системой инноваций. Производные показатели в GII имеют примерно одинаковые значения Score. Влияние исходных показателей усредняется.
3. Разработан комплекс ЛВ-моделей для оценки, анализа и управления системами инноваций стран, регионов, предприятий.
4. Разработана ЛВ-модель LP LGII, в которой значения оценок для производных событий-показателей на разных уровнях зависят от числа событий и их вероятностей и могут быть использованы для анализа и управления путем распределения ресурсов на изменение оценок.
5. Принятый в настоящее время GII и предложенный LP GII не рассматривают всех аспектов эффективного управления системой инноваций страны. Неясно, что делать для улучшения качества системы инноваций, и какова роль государства, бизнеса, ученых и общества в решении проблемы.
6. Разработана индикативная ЛВ-модель опасности системы инноваций; расчетами установлен большой риск опасности системы инноваций страны P=0.898, что свидетельствует о необходимости реформ в образовании, науке и экономике.
7. Разработана гибридная ЛВ-модель риска неуспеха системы инноваций; расчетами установлен большой риска неуспеха системы инноваций P=0.631, что также свидетельствует о необходимости реформ в образовании, науке и экономике; построение и анализ гибридных ЛВ-моделей риска -- является первоочередной задачей по совершенствованию систем инноваций.
8. Сравнительная оценка качества систем инноваций России, Финляндии, Швейцарии, США и Китая по GII и LP GII показала адекватность LP GII.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет

ПОДХОД К ОЦЕНКЕ ЗАЩИЩЁННСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

Возросшая сложность компьютерных сетей и механизмов защиты, увеличение количества уязвимостей пользователей, а также возможностей по реализации атак обуславливает необходимость разработки мощных автоматизированных средств (систем) анализа защищённости. В аппаратном и программно-техническом срезе эти проблемы решаются, существуют разработки систем анализа защищённости, в то же время эти средства, как правило, не учитывают или учитывают частично поведение пользователей. В последнее время существенная часть инцидентов нарушения информационной безопасности происходит при применении методов социальной инженерии.

Общая цель направления исследований заключается в построении оценки защищённости персонала информационных систем от социоинженерных атак. В докладе будет представлена формальная модель злоумышленника и входящая в неё модель профиля компетенций злоумышленника, на основании которых будет построена многофакторная оценка вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя. Построение оценки достигается за счёт агрегирования сведений о более широком круге факторов, влияющих на оценку вероятности успеха социоинженерного атакующего воздействия злоумышленника, и развития моделей комплекса «информационная система — персонал — критичные документы».

Будет представлен комплекс «критичные документы — информационная система — персонал — злоумышленник», а также модель пользователя информационной системы, включающая в себя модель профиля уязвимостей пользователя и модель злоумышленника, включающая в себя модель профиля компетенций злоумышленника. Будет предложен подход к формализации профиля компетенций злоумышленника и расчёту вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя с использованием определённого типа атаки и уязвимости.

Багрецов Г.И., Азаров А.А., Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет

ПОДХОД К ПОСТРОЕНИЮ ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ

В современном мире проблемы информационной безопасности человека становится всё актуальнее. Преступления, совершаемые с помощью компьютерных систем в виртуальном пространстве, происходят чаще, приносят большие убытки и требуют больше ресурсов и времени для их расследования. Наряду с ростом числа программно-технических атак, средства защиты от которых всё более совершенствуются, для нарушения информационной безопасности компаний также применяются социоинженерные атаки. Технической безопасности обычно уделяется достаточно много внимания, а наиболее уязвимым элементом информационных систем остаётся человек.

На сегодняшний день уже разработаны средства для определения вероятности успешности социоинженерной атаки злоумышленника. Однако, для корректного прогноза необходимо правильно оценить личностные характеристики пользователей информационной системы. В предыдущих исследованиях были определены различные типы уязвимостей, которыми может воспользоваться атакующий. Однако остаётся нерешённой проблема получения достоверной информации о пользователе. Кроме того, данную информацию необходимо должным образом структурировать и правильно трактовать.

Исследование посвящено выявлению методик извлечения знаний о пользователях информационной системы из их профилей в социальных сетях. Существует гипотеза о том, что можно построить профиль уязвимостей пользователя на основании анализа его активности в социальных сетях. А именно посредством анализа его списка друзей, сообществ, записей и комментариев, а также иных материалов.

Березин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СИНТЕЗ ВТОРИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ: ПЕДЖИНАЦИЯ АЛГОРИТМА ГЕНЕРАЦИИ МНОЖЕСТВА МИНИМАЛЬНЫХ ГРАФОВ СМЕЖНОСТИ

Последние исследования показывают, что генерация множества вторичной структуры “в лоб” невозможна в связи с возрастающим объемом хранимых данных при росте количества вершин. Данная статья посвящена решению данной проблемы. Все предполагаемое множество делится на блоки одинакового размера и вычисления откладываются до того момента, пока не понадобится их результат.

Бирилло А.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ СОГЛАСОВАННОСТИ ОЦЕНОК ИСТИННОСТИ В ЛОКАЛЬНОМ АПРИОРНОМ И АПОСТЕРИОРНОМ ВЫВОДЕ В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ: ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ

Алгебраические байесовские сети являются одним из относительно новых представителей класса вероятностных графических моделей для представления баз знаний с неопределенностью. Математической моделью фрагмента знаний в алгебраической байесовской сети выступает идеал конъюнктов.

Задача априорного вывода в алгебраических байесовских сетях заключается в построении вероятностной оценки пропозициональной формулы, не вошедшей в число заданных. При этом построение ведется с учетом известных вероятностных оценок истинности пропозициональных формул.

Задача апостериорного вывода разбивается на две подзадачи: оценка вероятности поступления свидетельства (детерминированного, стохастического или неточного) и пропагация свидетельства (детерминированного, стохастического или неточного) в фрагмент знаний, что влечет за собой переозначивание оценок вероятностей в рассматриваемом фрагменте знаний. При этом исходные фрагменты знаний в алгебраических байесовских сетях являются непротиворечивыми (согласованными).

В рамках данной работы рассматривается вопрос согласованности локального логико-вероятностного вывода в алгебраических сетях. Была поставлена цель разработки набора тестов для априорного и апостериорного вывода и анализа результатов на согласованность. Построение велось на все виды свидетельств: детерминированное, стохастическое и неточное. Тестирование было проведено с помощью двух подходов: математического и программного. Математический подход основан на ручной проверке с элементами компьютерных вычислений (например, для решения задач линейного программирования в среде MAPLE). Программный подход базируется на комплексе программ «AlgBNModeller», разработанного на языке C#, в котором все составленные тесты были протестированы средствами комплекса.

В ходе данного исследования было разработано методическое пособие к комплексу программ «AlgBNModeller», которое охватывает теоретические сведения о решении задач локального априорного и апостериорного вывода для трех типов свидетельств (детерминированного, стохастического или неточного), а также практические результаты, полученные в ходе данного исследования. Также оно содержит краткое руководство пользования комплексом для решения задач локального априорного и апостериорного вывода.

Волков Н.В., Григорьев Д.А
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПРИМЕНЕНИЕ АОП-РЕФАКТОРИНГА В КРУПНЫХ CMS ПРОЕКТАХ ПРИ ПОМОЩИ ASPECT.NET

Разделение проекта на отдельные модули стало неотъемлемой частью процесса его разработки, при этом реализация некоторых видов функциональности невозможна в рамках одного модуля. В качестве наиболее часто встречающихся примеров могут служить вопросы безопасности (организация доступа, прав пользователей и защита данных), надежности (выполнение пред- и пост-условий в модулях, обработка ошибок) и другие. В терминологии аспектно-ориентированного программирования (АОП) такой код называется сквозной функциональностью. Характерной проблемой сквозной функциональности является реализация изменений, в случае необходимости, в большом количестве участков кода. Аспектно-ориентированный подход предлагает удобное решение проблемы сквозной функциональности, выделением сквозной функциональности в единственный модуль (аспект).

Рефакторингом называют изменение написанного ранее кода, не влияющее на его поведение, направленное на улучшение структуры кода. АОП-рефакторинг предполагает ряд аспектно-ориентированных преобразований, направленных на выделение из целевого кода сквозной функциональности в аспекты. Помимо решения проблемы внесения изменений в большое количество

участков программы, грамотный АОП-рефакторинг позволяет использовать готовую функциональность повторно в других проектах или участках кода без внесения кардинальных изменений. Также АОП-рефакторинг упрощает процесс отладки и поддержки уже созданного кода.

Для реализации АОП-рефакторинга на платформе .NET был использован АОП-инструмент Aspect.NET. С помощью Aspect.NET можно определять аспекты в отдельных библиотеках классов, а затем вплетать вызовы их методов в заданные места целевой сборки. Реализация аспекта в Aspect.NET осуществляется статическими методами, которые затем будут вставлены в заданные точки внедрения в сборке проекта, либо аспектным наследником, заменяющим своего родителя в целевом проекте.

АОП-рефакторинг может быть применим как в небольших, так и в крупных проектах для улучшения качества некоторых модулей, однако наибольшую эффективность этот метод показывает при использовании его в крупных проектах. Целью работы была разработка АОП-рефакторингов крупных CMS-проектов при помощи Aspect.NET. В качестве цели рефакторинга были выбраны open-source CMS-проекты под названием n2cms и Orchard, в рамках данной работы было произведено некоторое количество рефакторингов:

Для n2cms:

1. Извлечение методов, выполняющих функционально схожую работу. Приведен аспект, обновляющий записанные значения в базе данных.
2. Перенос обработки исключений в два аспекта, реализующих чтение событий из журнала и обработку изменения местоположения файла.
3. В отдельный аспект вынесены методы, отвечающие за протоколирование вызова определенного метода.

Для Orchard:

1. Перенос обработки исключений в аспект, реализующий чтение событий из журнала.
2. При протоколировании методы содержат одинаковый код, который можно вынести в отдельный метод. Строки, отвечающие за работу с журналом событий, выносятся в отдельные действия.
3. Функциональность методов, выполняющих форматирование различных типов данных, была перемещена в аспект. Полученные действия также можно использовать вторично.

В классе ContainerService находятся методы, которые взаимодействуют с контейнерами. Эти методы были вынесены в отдельный аспект.

Оценка полученных результатов проводилась при помощи метрик Maintainability Index, содержащихся в Visual Studio и показывающих качество кода. В каждом из случаев были получены положительные результаты, например, индекс качества целевого класса для записи в базу данных улучшился на 20%, а индексы других рефакторингов более чем на 10%. Таким образом, следует отметить возможность и перспективность использования АОП-рефакторингов в крупных проектах. Использование этого метода позволяет сократить расходы на тестирование и сопровождение кода, а также дает возможность реального повторного использования сквозной функциональности.

Григорьева А.В., Григорьев Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

БЕСШОВНАЯ ИНТЕГРАЦИЯ СРЕДСТВ ПРОВЕДЕНИЯ СОЦИАЛЬНЫХ ОПРОСОВ С ASP.NET MVC ВЕБ-ПРИЛОЖЕНИЯМИ НА ОСНОВЕ ASPECT.NET

В современном обществе веб-приложения являются главным способом удовлетворения информационных потребностей человека: новостные сайты, социальные сети, электронная почта и т.п. Одновременно с веб-приложениями работает множество людей из разных слоев, социальных и возрастных групп. Становится очевидным тот факт, что сбор информации для проведения социальных исследований с помощью веб-приложений является актуальной задачей.

Одной из надежнейших методик проведения социальных исследований является анкетирование респондентов, когда специалисты составляют список вопросов, а представители целевой аудитории дают на них свои ответы. Однако приходится учитывать тот факт, что во время опроса образ мыслей и, соответственно ответы, индивидуума могут не соответствовать его обычному состоянию. Помимо прочего, причиной может являться непривычная обстановка, которая меняет привычные паттерны поведения. В связи с этим, организация социального опроса на каком-либо веб-ресурсе должна соответствовать его стилю, дизайну и информационному наполнению, избегая при этом перенаправления на какой-либо другой сайт.

Следовательно, чтобы анкетирование было максимально комфортным для пользователя веб-приложения, его разработчик должен добавить требуемую функциональность. В этом смысле функциональность анкетирования можно рассматривать как “сквозную”, в том смысле, что ее визуальные элементы переплетаются со многими страницами сайта, а управляющий код этих страниц должен обрабатывать от них события. Все это повышает общую сложность веб-приложения, увеличивает число зависимостей его классов и ухудшает их связность.

Авторами был предложен подход улучшения качества исходного кода ASP.NET MVC веб-приложений за счет бесшовного добавления функциональности проведения социальных опросов. Для этого применяется разработанная в СПбГУ система аспектно-ориентированной разработки программ Aspect.NET. Данная система позволяет реализовывать сквозную функциональность в отдельном проекте (аспекте) и вплетать ее вызовы в нужные точки целевого кода на бинарном уровне MSIL-инструкций, что дает возможность не менять целевой проект. При этом аспект имеет доступ к программному контексту точки внедрения, что позволяет получать и менять состояние целевой программы, в то время как ее исходный код не зависит от аспекта.

Суть рассматриваемого метода, заключается в том, что весь, необходимый для анкетирования код, выносится в отдельный проект, который может быть затем повторно использован. Отмечается, что необходимые для анкетирования структуры данных комбинируются в отдельный класс модели, а разметка визуальных элементов переносится в ascx-компонент, который связывается с этой моделью. Далее к логике целевого контроллера добавляется обработка действия для анкетирования путем создания “замещающего” наследника. В этом действии происходит наполнение данными модели для анкетирования и передача ее ascx-компоненту для отображения. Для того, чтобы целевое приложение получило новую функциональность, необходимо в декларативный .aspx-код вставить вызов соответствующего действия контроллера и с помощью Aspect.NET интегрировать аспектный проект в целевое приложение. Таким образом, решена проблема запутанного кода, а именно: логика анкетирования содержится только в одном месте - аспекте, а удалить ее можно простым удалением декларативных элементов и игнорированием данного аспекта.

Искрич Д.П, Григорьев Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПРИМЕНЕНИЕ ДЕРЕВЬЕВ РЕШЕНИЙ В ОБЛАСТИ БИРЖЕВОГО ТРЕЙДИНГА

Любой трейдер стремится выработать свою торговую систему, которая определяет в какое время и с какими параметрами необходимо покупать или продавать определенные инструменты. При принятии решения наиболее часто применяется технический анализ, предлагающий множество показателей и индикаторов, основанных на поведении графика цены в прошлом. В этом случае торговые правила формируются на сочетаниях показателей, их текущих и прошлых значений.

Существует множество алгоритмических подходов для формирования торговой системы, в том числе методами искусственного интеллекта: нейронные сети, генетические алгоритмы, агентный подход и т.д. При этом наибольшую прозрачность и простоту обоснования полученного правила предоставляют деревья принятия решений, которые способны.сформировать правила для сигналов покупки/продажи в виде списка логических формул в конъюнктивной нормальной форме.

Деревья при таком подходе представляют из себя набор нетерминальных и листовых узлов. Существует большое количество работ посвященных методам генерации подобных деревьев и способам организации структур данных. В данной работе используются бинарные деревья, при этом на нетерминальный узел ставится предикат определяющий переход к новому узлу. Предикат возвращает значение из множества {true, false}, что определяет переход к правому или левому потомку. При этом сам предикат представляет из себя проверку значений какой-либо индикатора технического анализа. Таким образом начиная с корневого предиката, мы рано или поздно спустимся к листовому узлу, который будет представлять из себя сигнал покупки или продажи.

Получение оптимальных деревьев принятия торговых решений сводится к применению следующего генетического алгоритма:

1. Начальная популяция формируется случайным образом, предикат узла каждого дерева состоит из случайно выбранного наименования индикатора и его случайно выбранного значения.
2. Вычисляются значения целевой функции для каждой особи из популяции, путем подсчета прибыли на исторических данных после бэк-теста ее дерева решений.
3. Отбор деревьев для следующего поколения методом рулетки.
4. Применение генетических операторов для создания новых потомков и для мутации существующих.
5. Повторение шагов 2-4 до тех пор пока не наступает заданное поколение N.

Для тестирования системы были выбраны акции 4 компаний IT индустрии: Apple, Inc, International Business Machines, Oracle Corporation, Microsoft Corporation. Средний результат прибыли на данных в интервале 30 января 2014-го года - 30 января 2015-го года составляет 22.31%, при форвард тестировании был зафиксирован средний результат в 3.2%, однако на данный момент отсутствует модуль подсчета налога за транзакции и учет возможных временных задержек.

Данная система не исключает наличие в итоговом дереве решений и правил, определенных пользователем и основанных на пересечении близких по своей природе индикаторов. Таким образом, после заданного количества итераций мы получаем наиболее оптимальное дерево, которое можно использовать в качестве советника для последующей торговли.

Каспрук.Н.С.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»
АНАЛИЗ ИЗМЕРЕНИЙ ЦЕННОСТИ И СТРАТИФИКАЦИИ КЛИЕНТОВ ОТЕЛЕЙ НА ОСНОВЕ ОНЛАЙН-ДАННЫХ. СЛУЧАЙ САНКТ-ПЕТЕРБУРГА

Интернет в настоящее время является преобладающим средством для выбора отелей и для сбора информации о них. Более 84% потребителей обращаются к рекомендательным системам, основой которых являются отзывы предыдущих клиентов, прежде чем делать покупки. Одним из важнейших факторов роста популярности данных систем – является возможность непосредственного eWOM (electronic word-of-mouth) взаимодействия: неформальной он-лайн передачи информации от человека к человеку относительно бренда, продукта, организации или службы.

В прикладных маркетинговых исследованиях анализ тональностей отзывов уже некоторое время является стандартным методом, позволившим увеличить точной предсказательной аналитики и анализа качества услуг.

Вместе с тем, отзывы являются важным эмпирическим материалом и для задач социокомпьютинга, в частности, анализа социального конструирования измерений ценности и доверия в многопользовательских системах.

Настоящее исследование построено на выборке отзывов об отелях Санкт-Петербурга и метаданных, в том числе о категории и расположении отеля. С использованием методов обработки естественного языка и машинного обучения рассмотрены конструируемые клиентами измерения ценности для отелей, относящихся к разным ценовым категориям.

Показано, что стратификация отелей ассоциирована с разницей в важности измерений ценности, а также с демонстративным потреблением городских впечатлений.

Построен прототип рекомендательной системы, учитывающий эти факторы.

Левенец Д.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ДЕКРЕМЕНТАЛЬНЫЙ СИНТЕЗ ВТОРИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ: СТАТИСТИЧЕСКАЯ ОЦЕНКА СЛОЖНОСТИ

Рассмотрена задача декрементального синтеза вторичной структуры алгебраических байесовских сетей. Выполнен статистический анализ сложности декрементального алгоритма в сравнении с улучшенным декрементальным алгоритмом.

Статистические эксперименты визуализированы в виде графиков.

Мальчевская Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
АРХИТЕКТУРА БИБЛИОТЕКИ ALGBNMODELLER: ПРЕДСТАВЛЕНИЕ АЛЬТЕРНАТИВНЫХ ФРАГМЕНТОВ ЗНАНИЙ

Алгебраические байесовские сети — отечественная разработка, предложенная В.И. Городецким — представляют собой модель баз фрагментов знаний с неопределенностью, классической математической моделью которых выступает идеалов конъюнктов с заданными над ними интервальными либо скалярными вероятностными оценками. Конъюнкты, как и другие формулы, задаются над некоторым фиксированным алфавитом. Существуют также альтернативные способы задания модели фрагмента знаний. Фрагмент знаний может быть представлен как идеал дизъюнктов, а также как набор квантов. В некоторых случаях такие представления знаний существенно удобнее, в частности, при формализации знаний экспертов и формализации ограничений. Для работы с подобными структурами необходимы подходящие программные средства и программное обеспечение.

Разработана библиотека AlgBNModeller по осуществлению локальных априорного и апостериорного выводов над фрагментами знаний, которые могут быть заданы над различными множествами, а также могут иметь как скалярные, так и интервальные оценки вероятности истинности элементов. Библиотека позволяет создавать как классические фрагменты знаний, так и альтернативные.

В докладе представлена часть библиотеки, отвечающая за создание фрагмента знаний над набором квантов и идеалом дизъюнктов. Приведены диаграммы зависимостей интерфейсов и других структур, отвечающих за рассматриваемую функциональность.

Мусабиров И.Л., Поздняков С.И., Бахитова А.А., Суворова А.В.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»,
Санкт-Петербургский институт информатики и автоматизации РАН

ПРОЕКТИРОВАНИЕ СОЦИАЛЬНОЙ СИСТЕМЫ ГЕЙМИФИКАЦИИ КУРСА С ОНЛАЙН-КОМПОНЕНТОЙ

Массовое распространение онлайн- и смешанных курсов привело к появлению новых масштабных источников данных о поведении студентов и, вместе с тем, поставило новые вопросы по созданию и удержанию их мотивации к успешному завершению курсов.

Одним из популярных средств привлечения и удержания пользователей онлайн-сервисов, в том числе и образовательных, является геймификация -- внедрение игровой логики в неигровые контексты.

Стандартными инструментами геймификации влияющими на мотивацию, считаются очки (points), бэйджи (badges) и рейтинги пользователей (leaderboards). Бэйджи выступают индикаторами достижения определенной цели и обычно выдаются как награда за совершенное действие или поощрение к совершению нового. Хотя исследования ряда ученых, в том числе Papastergiou, Domínguez, Anderson и Huttenlocher показывают некоторую эффективность бейджей в образовательных сервисах, важными вопросами остается долговременная мотивация студентов, а также то, что контрольной группой в таких исследованиях часто выступают онлайн-сервисы без применения геймификационных инструментов, то есть более высокая по сравнению с ними мотивация может являться недостаточной по меркам успешных традиционных форм обучения.

Отдельный интерес вызывает и использование геймификационных систем в смешанных курсах, где традиционные инструменты мотивации могут как усиливать, так и конкурировать с новыми, завязанными на игровые элементы. Перспективным представляется подход к системному проектированию оценочно-мотивационной системы таких курсов на основе применения методов образовательной аналитики к данным о взаимодействии студентов с виртуальным образовательным окружением.

В докладе рассмотрен анализ поведения студентов в смешанном курсе по анализу данных с традиционной и онлайн-компонентами на основе журналов поведения в виртуальном образовательном окружении.

Сконструированы три группы метрик, образующие следующие измерения: активность взаимодействия с виртуальной средой и программным интерпретатором RStudio, коммуникационная активность на форуме, и характеристики сетей дружбы студентов. Определены основные стратегии студентов по взаимодействию с виртуальным образовательным окружением и их связь с образовательным результатом.

На основе принципов дизайна стимулов, предложена схема частичной геймификации курса, учитывающая социальное взаимодействие студентов, и обсуждено её взаимодействие с традиционной системой оценивания.

Нестеренко А. В., Мусабиров И. Л.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»

АНАЛИЗ СПЕЦИАЛИЗАЦИИ ИТ-РЫНКА НА ОСНОВЕ ДАННЫХ ОНЛАЙН-РЕКРУТИНГА

Усиливающаяся миграция в Веб функции первоначального поиска кадров по ИТ-специальностям за счет сайтов-«посредников», снижающих затраты на поиск потенциальных кандидатов, в частности рекрутинговых сайтов и бизнес-ориентированных социальных сетей, помимо существенного влияния на устройство процесса рекрутинга, даёт возможность проанализировать структуру рынка на масштабных эмпирических данных.

В частности, доступными для анализа становятся данные о формировании и изменениях конкретных профессиональных ролей -- наборов востребованных технологических навыков. Кроме того, сопоставление спроса и предложения в разрезе этих ролей позволяет определить несоответствия (mismatch) потребностей индустрии и компетенций соискателей, предоставляя первой фактическую базу для кадровой стратегии, а вторым -- “карту” для повышения собственной стоимости на рынке труда за счет планирования развития компетенций и навыков, востребованных работодателями.

В нашей работе был использован срез данных резюме и вакансий, доступный на одном из онлайн-площадок по поиску работы в сфере ИТ. Основой анализа выступили наборы тегированные навыки соискателей и работодателей.

Используя методы машинного обучения и сетевого анализа, были получены иерархии навыков отдельно для вакансий и кандидатов, описывающие структуру рынка технологий, получены кластеры навыков, характеризующие как области универсальных требований, так и области специализации. На основе полученных наборов был проведен анализ спроса и предложения с помощью теста логарифмического отношения правдоподобия для таблиц сопряженности.

Были выявлены зоны дисбаланса спроса и предложения. Так, недостаточно представлены навыки работы с наборами библиотек разработки AngularJS, Java Spring, React.JS, реляционной СУБД PostgreSQL. Кроме того, хуже представлены в резюме “инфраструктурные” навыки, связанные с организацией разработки, в том числе система управления версиями Git, архитектура веб-сервисов Rest. В то же время базовые навыки разработки представлены в избытке: для HTML, CSS, PHP предложение значимо превышает спрос.

Несмотря на необходимость принять во внимание разницу в языке описания навыков и требований в вакансиях и резюме, а также необходимость валидации на других источниках данных, результаты исследования проливают свет на специализацию ИТ-рынка на микроуровне.

Поздняков С.И., Воскресенский В.М., Карепин В.В., Кузнецова А.Д., Федюнина А.А., Мусабиров И.Л.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»

ТЕМАТИЧЕСКИЙ КОНТЕКСТ В КАРТИРОВАНИИ ВЕБ-ПРИСУТСТВИЯ И НАУЧНО ДЕЯТЕЛЬНОСТИ РОССИЙСКИХ ВУЗОВ. МЕТОДИКИ АНАЛИЗА

Несмотря на растущую востребованность рейтингов как инструмента ранжирования и оценки результатов деятельности университетов, они вызывают значительный объем критики. Как правило, критике подвергаются показатели, составляющие рейтинг, в том числе показатели, основанные на опросах экспертов, а также веса отдельных показателей и способы агрегации данных. Альтернативные подходы, такие как альтметрики и вебометрики, основывающиеся на измерении веб-присутствия вузов, вызывают растущий интерес, однако не учитывают контекст и специфику веб-присутствия. Таким образом, возникает необходимость разработки способов анализа веб-присутствия и научной деятельности вузов, дающих достаточно степеней свободы для учета их специфики, но также и обеспечивающих возможность сопоставлений.

Представленность в интернете, с одной стороны, является отражением результатов научной, образовательной, экспертной и иной деятельности вуза, а с другой стороны, является необходимой составляющей для продвижения университетов во внешней средне. Существует несколько основных подходов к оценке "реальной" («оффлайновой») деятельности университетов на основании онлайн-данных, общей чертой которых является анализ входящих ссылок на домен университета (Web Impact Factor), результатов выдачи поисковых движков. Исследования показывают, что данный метод способен достаточно точно оценить размах научной деятельности университета, не используя напрямую данные из библиометрических баз Web of Science и Scopus. Данный подход называют вебометрическим: необходимо отметить, что вебометрики являются скорее комплементарными по отношению к уже сложившимся библиометрическим показателям. Ссылки отражают различные аспекты «видимости» — партнерства, доступность информации иностранным и российским абитуриентов «домашнего» и других регионов, включенность в новостной поток, сведения о научных мероприятиях. Вместе с тем, простая агрегация ссылок не делает различений между их типами. В работе описывается способ построения карт университетов, сочетающих наукометрические показатели по основным релевантным для России индексам (Web of Science Core Collection, Russian Science Citation Index, Scopus, РИНЦ) и вебометрики - показатели представленности вузов в Интернете, на сайтах ключевых компаний-работодателей и партнеров и СМИ. Тогда как традиционные вебометрики предполагают акцент на интегральном показателе веб-присутствия, введение локального контекста - изучение ссылок из ключевых федеральных и региональных СМИ и топа работодателей и партнеров - позволяет произвести более подробную оценку деятельности университетов.

В работы мы попытались совместить основные измерения, через которые может быть измерена деятельность университетов:

- библиография: данные о публикациях университета (Web of Science Core Collection, Russian Science Citation Index, Scopus, РИНЦ);
- связи с ключевыми работодателями и партнерами региона;
- представленность в СМИ: количество упоминаний на сайтах основных СМИ.

Для анализа тематического контекста, на предварительном перечне вузов экономико-управленческого профиля Северо-Западного региона РФ, входящие ссылки и сайты работ были проанализированы с применением тематического моделирования на основе алгоритма Latent Dirichlet Allocation. Таким образом получены тематические контексты, расширяющие описание характера деятельности университетов. Кроме того, проанализировано положение университетов в пространстве метрик с использованием методов снижения размерности. Предложенный подход позволяет преодолеть ограничения узкого стратификационного взгляда, основанного на ранжировании, в пользу более глубокого понимания взаимного «расположения» университетов в контексте тематик научной деятельности и вовлеченности в локальные связи.

Столярова В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ НА ОСНОВЕ КОПУЛ ДЛЯ ПОСТРОЕНИЯ ОЦЕНКИ ИНТЕНСИВНОСТИ УГРОЗООБРАЗУЮЩЕГО ПОВЕДЕНИЯ ИНДИВИДА ПО ДАННЫМ О ОСЛЕДНИХ ЭПИЗОДАХ

Математическое моделирование показателей поведения индивида, связанного с риском распространения неизлечимых заболеваний (к примеру, ВИЧ), является актуальной задачей современной эпидемиологии. Математические модели позволяют как убыстрить и упростить расчет эпидемических показателей заболевания, так и оценивать целесообразность различных способов интервенции. Оценка интенсивности рискованного поведения важна при расчете нагрузки, которую дает заболевание на социальную и экономическую сферы жизни общества (disease burden). Согласно исследованиям Всемирной Организации Здравоохранения, ВИЧ и СПИД имеют одну из лидирующих позиций среди заболеваний, ведущих к нетрудоспособности и сокращению времени жизни (5 порядковое место в мире и 2-4 в России).

Как показывают пилотные опросы, респондент может достоверно привести информацию о нескольких последних эпизодах поведения и/или рекордных интервалах между эпизодами поведения. Такую информацию можно представить в виде нескольких зависимых непрерывных случайных величин, которые соответствуют длинам интервалов между эпизодами. Был разработан ряд теоретических моделей, позволяющих получить оценку интенсивности поведения по таким данным. Практическое применение таких моделей связано с построением байесовской сети доверия, отражающей структуру взаимосвязей переменных (с узлом-родителем в такой сети связана интенсивность поведения, а с узлами детьми --- переменные длин интервалов).

Основным недостатком модели БСД является потеря информации при дискретизации переменных длин интервалов. В работе представлены две модели для построения оценок интенсивности поведения по сверхкоротким данным, которые позволяют обойти указанный недостаток. Основой для них служат модель лозы (vine) и непрерывная непараметрическая байесовская сеть доверия, которые относятся к классу вероятностных графических моделей.

Модель лозы представляет собой вложенное множество деревьев, узлами последующего являются ребра предыдущего. С узлами первого дерева связаны переменные интенсивности и длин интервалов, однако для работы моделей не требуется их дискретизация. Математической моделью причинно-следственных связей модели служит аппарат копул. Копулы не изменяются при монотонном преобразовании случайных величин, связанных ею, и однозначно определяют ранговые коэффициенты корреляции. Если задан ранговый коэффициент корреляции и тип копулы, то однозначно определен и параметр копулы. Таким образом, с ребрами представленных моделей связаны коэффициенты ранговой корреляции (частичной ранговой корреляции для деревьев порядка выше первого), которые могут быть определены экспертным путем.

Непараметрическая непрерывная байесовская сеть доверия (ННБСД) представляет собой направленный ациклический граф, узлы которого также представляют собой непрерывные переменные (длины интервалов и интенсивность), а ребра --- коэффициенты (частичной) ранговой корреляции.

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК ТЕСТОВЫХ ДАННЫХ В МОДЕЛИ ОЦЕНИВАНИЯ ХАРАКТЕРИСТИК СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ

В ряде отраслей наук растет интерес к изучению количественных характеристик социально-значимого поведения. Задачи оценивания интенсивности социально-значимого поведения респондентов возникают во многих отраслях социологических, психологических, маркетинговых исследований. Однако применение прямых методов часто невозможно, что требует развития косвенных методов оценки.

В докладе представлены результаты тестирования разработанной модели для оценивания характеристик социально-значимого поведения на данных о поведении в социальной сети. Предложенная байесовская сеть доверия, основанная на данных о нескольких последних эпизодах поведения, позволяет объединять в одной модели как знания экспертов о характере поведения, так и статистические данные о длинах интервалов между последовательными эпизодами рассматриваемого поведения. Однако тестирование модели сталкивается с рядом ограничений: в частности, фактические сведения об интенсивности поведения (необходимые для проверки правильности оценки) за определенный, часто достаточно длительный промежуток времени получить сложно, а иногда и невозможно (например, узнать точно число незащищенных сексуальных контактов за полгода для оценки риска передачи ВИЧ-инфекции).

В качестве реальных данных о поведении рассмотрены сведения о моментах публикации пользователем поста на собственной стене в социальной сети ВКонтакте. Для каждого из 1500

случайно выбранных пользователей социальной сети были собраны данные о длинах интервалов между тремя последними эпизодами публикации постов, а также о длинах максимального и минимального интервалов между публикацией постов за предшествующие полгода. Индивидуальные оценки интенсивности, полученные согласно предложенной модели, принадлежат тем же интервалам значений интенсивности, что и фактическое значение, в среднем в 91% случаев (при разбиении возможных значений интенсивности на восемь интервалов). Показано, что в целом по группе апостериорное распределение случайной величины, соответствующей интенсивности, статистически не отличается от распределения фактических значений. Таким образом, на указанных данных о поведении в социальной сети модель имеет хорошие показатели качества при сравнении с фактическими значениями интенсивности поведения.

Торопова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ СОГЛАСОВАННОСТИ ДАННЫХ В РАСШИРЕННОЙ МОДЕЛИ ОЦЕНКИ СОЦИАЛЬНО-ЗГНАЧИМОГО ПОВЕДЕНИЯ

Одно из главных направлений социокомпьютинга – это анализ социальных сетей. В социальных сетях пользователи могут совершать различные действия, например, публиковать посты, посылать друг другу сообщения и т.д. Эти действия представляют собой социально-значимую активность, одна из характеристик которой – интенсивность этого поведения. С помощью анализа интенсивности социально-значимой активности можно предсказывать дальнейшее поведение как определенного пользователя, так и каких-то групп пользователей. Применение таким прогнозам можно найти в различных областях (социология, маркетинг и т.д.).

Для анализа интенсивности социально-значимой активности А.В. Суворовой была предложена модель на основе байесовских сетей доверия. В докладе рассматриваются расширения данной модели для оценки согласованности данных, полученных от респондентов.

Харитонов Н.А., Мальчевская Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЛОКАЛЬНЫЙ АПРИОРНЫЙ ВЫВОД В АБС: АВТОМАТИЗАЦИЯ АНАЛИЗА ПРОПОЗИЦИОНАЛЬНОЙ ФОРМУЛЫ

Алгебраические байесовские сети (АБС) -- вероятностные графические модели, которые представляются ненаправленными графами с идеалами конъюнктов в узлах. Рассматриваются различные виды логико-вероятностного вывода: поддержание непротиворечивости, априорный и апостериорный, глобального или локального уровня. В случае глобального вывода действия производятся над всей сетью, в то же время при локальном выводе операции привязаны к конкретному узлу, называемому фрагментом знаний.

Локальный априорный вывод заключается в поиске вероятности произвольной пропозициональной формулы, на основе имеющихся вероятностей рассматриваемого фрагмента знаний. Для этого необходимо преобразовывать входную пропозициональную формулу, представленную в виде строки, в характеристический вектор квантов, а далее вычислить вектор коэффициентов в разложении рассматриваемой формулы по конъюнктам фрагмента знаний (ФЗ). Автоматизации этих преобразований и посвящена данная работа.

Весь процесс разбивается на несколько отдельных шагов. При помощи модифицированного алгоритма получения обратной польской записи, строится дерево разбора строки. Далее, используя рекурсивный спуск по построенному дереву, вычисляется характеристический вектор совершенной дизъюнктивной нормальной формы для исходной формулы. Он преобразуется в вектор коэффициентов в разложении входной формулы по элементам фрагмента знаний. Вероятность формулы получается в результате перемножения вектора коэффициентов и вектора вероятностей истинности конъюнктов ФЗ. Данное решение имеет программную реализацию, а также используется в библиотеке локального логико-вероятностного вывода в АБС AlgBNModeller.

Шиндарев Н.А., Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет
ПОСТРОЕНИЕ ВЕРОЯТНОСТНОЙ ГРАФИЧЕСКОЙ МОДЕЛИ ДЛЯ ОЦЕНКИ УСПЕШНОСТИ СОЦИОИНЖЕНЕРНОЙ АТАКИ

Одна из существенных задач обеспечения информационной безопасности сегодня, остающаяся по-прежнему нерешённой, заключается в анализе защищённости пользователей от социоинженерных атак. На сегодняшний день уже предложен ряд алгоритмов, использующих для оценки степени защищённости модели комплекса: «информационная система – персонал – критичные документы». Такая оценка строится на основании профиля уязвимостей пользователя.

Объектом исследования данной работы является разработанный подход к анализу распространения социоинженерной атаки злоумышленника среди пользователей информационной системы, представленного в виде графа социальных связей. В ходе исследования было выдвинуто предложение о частичной генерации всевозможных путей распространения социоинженерной атаки злоумышленника внутри полных подграфов графа социальных связей пользователей информационной системы: примером таких подграфов являются контролируемые зоны и отделы компаний. Практическая реализация данной идеи позволяет за счет хранения лишней информации в памяти уменьшить временные затраты при новых попытках просчитать возможные действия злоумышленника.

РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, ГРИД-ТЕХНОЛОГИИ

Воробьев В.И., Петров М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

МЕТОДЫ КОНВЕРГЕНЦИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И БОЛЬШИХ ДАННЫХ

Опыт переноса информационных услуг в виртуальную инфраструктуру показывает свою эффективность и надежность, а также возможность более широкой виртуализации технологий. Так, перспективным направлением развития является включение виртуальных ресурсов в единую среду управления. Одна из целей интеграции облачной платформы заключается в создании системы, управляющей существующими АИС виртуальных информационных сервисов, создании шаблонов виртуальных машин и унификации программной платформы.

Проведены эксперименты по расширению функциональности кластера СПИИРАН, включая развитие индивидуальных решений, использование разнообразных инструментальных средств и гипервизоров, что позволит снизить совокупную стоимость владения и обеспечить надежную систему управления виртуальными ресурсами. В данном случае обеспечивается горизонтальное масштабирование вычислительных ресурсов и виртуализация гетерогенных программных систем на одной аппаратной платформе. Уникальной характеристикой является поддержка вычислителей разного типа, включая стандартные микропроцессоры, потоковые вычислители на базе графических ускорителей и специализированные решения.

Конвергенция достигается за счет переноса – частичного или полного – функциональности оборудования с аппаратного уровня на программный, исполняемый на серверах общего назначения. Поэтому класс такого виртуализованного оборудования уже в меньшей степени определяется «железом», что позволяет на программном уровне обеспечить приложению именно те характеристики аппаратной платформы, какие ему необходимы в конкретный момент времени.

В основу конвергентной инфраструктуры на физическом слое, как было сказано, положена вычислительная ткань (fabric computing), эта технология в контексте повторяет Grid-системы, в частности, на многих проприетарных схемах присутствует Server Fabric. Показана роль больших данных в конвергентных структурах. Данные растут непредсказуемо, а точнее – предсказуемо растут неструктурированные данные. Одно из решений в работе с большими данными – переход к единому транспорту для передачи различных типов трафика, включающего консолидацию серверов ввода/вывода, и конвергенция на уровне ядра сети, которая реализуется на базе высокопроизводительных коммутаторов Ethernet.

Для конвергенции технологий обработки больших объемов накапливаемых данных можно использовать современные инструменты (например, Hadoop). Основной особенностью подобных инструментов является почти линейная горизонтальная масштабируемость (производительность системы почти линейно зависит от числа узлов кластера). Главным достоинством подхода является возможность анализировать и обрабатывать разно-структурированные данные, например, реляционные, XML, JSON, тексты и другие.

Князева К.О., Воеводский К.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ: ПОНЯТИЕ И ВИДЫ

Современное общество динамично развивается, а вместе с ним усложняется и его информационно-техническая структура – объемы данных, обрабатываемых в информационных системах, растут, сами информационные системы становятся всё «ветвистее» и приобретают всё больший территориальный разброс. Оперативное использование информации, находящейся на удаленном оборудовании, позволяет повысить эффективность управления, а также является одним из условий успешного экономического развития и конкурентоспособности организации. Такие реалии повлияли на развитие и широкое распространение распределенных информационных систем.

В настоящее время в литературе рассматривается большое количество толкований понятия «распределенная система». Наиболее точное было предложено Эндрю Стюартом Таненбаумом (A.S. Tanenbaum): «Распределенная система (РС) – это набор независимых компьютеров, который воспринимается его пользователями как единая последовательная система». Еще одно определение представлено в работе группы авторов: «Распределенными системами называются программно-аппаратные системы, в которых исполнение операций (действий, вычислений), необходимых для

обеспечения целевой функциональности системы, распределено (физически или логически) между разными исполнителями». В сфере вычислений под распределенной системой можно понимать программно-аппаратную систему, для конкретного практического применения, функционал которой распределен на различных узлах.

Произвести классификацию распределенных систем можно по различным признакам: по общему количеству элементов в системе, по уровню организации распределенных систем, по типу предоставляемых ресурсов, а также ряду других признаков.

По типу предоставляемых ресурсов различают:

- распределенные вычислительные системы (Computational Grid);
- распределенные информационные системы (Data Grid);
- семантический Грид (Semantic Grid).

Распределенные вычислительные системы характеризуются тем, что основным ресурсом в них является вычислительная мощность всей системы. Главным направлением развития систем данного типа является наращивание вычислительных мощностей системы, путем увеличения числа вычислительных узлов. Примером распределенных вычислительных систем являются кластеры. Распределенные информационные системы предоставляют вычислительные ресурсы для обработки больших объемов данных, для задач, не требующих больших вычислительных ресурсов. Семантический Грид предоставляет не только отдельные вычислительные мощности (базы данных, сервисы), но и совокупность вычислительных и информационных систем, для каждой конкретной предметной области.

По количеству элементов в системе различают следующие распределенные системы:

- кластер;
- распределенная система корпоративного уровня;
- глобальная система.

Распределенная система является кластером, если общее количество входящих в ее состав элементов не превышает несколько десятков штук. Распределенная система корпоративного уровня содержит в своем составе уже сотни, а в некоторых случаях, и тысячи элементов. Глобальной системой называется распределенная система с количеством элементов, входящим в ее состав, более тысячи. При этом, зачастую, элементы таких систем глобально распределены. Примером глобальной распределенной сети является Интернет, где в качестве предоставляемого ресурса выступает информационное поле.

В транспортной сфере эксплуатируются распределенные системы, в которых обрабатывается очень большой объем данных. К примеру, крупнейший игрок рынка транспортно-логистических услуг в России, компания Российские Железные Дороги, имеет в своем распоряжении три главных центра обработки данных (Москва, Санкт-Петербург, Екатеринбург) и множество вспомогательных. Рабочие места пользователей распределены по всей стране, они есть на каждой железнодорожной станции. В системе содержатся и обрабатываются колоссальные объемы данных, для которых требуются колоссальные вычислительные мощности. Как раз эти задачи и призваны решать распределенные системы.

Копыльцов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

РАЗРАБОТКА ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ДЛЯ ОБРАБОТКИ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ

Проблемы, связанные с обработкой слабо формализованной информации, поступающей от объекта исследования (технической системы), за приемлемое время актуальны, поскольку на основе поступившей информации необходимо принимать решения в ограниченные промежутки времени. Формализация информации, предполагается в первую очередь научной информации, – это процесс представления информации об объектах и процессах в формализованном виде, т.е. в некоторой форме, чаще всего математической, т.е. представление информации в виде формулы, соотношения, уравнения, дифференциального уравнения, системы дифференциальных уравнений в частных производных, алгоритма и т.д. При такой формализации она в дальнейшем может быть подвергнута эффективной обработке на компьютере. Поэтому, при поступлении новой информации пытаются ее формализовать, в первую очередь, таким образом, чтобы получились известные (подобные) математические формулы, уравнения, алгоритмы и пр. Формализация – это процесс и поэтому необходимо разрабатывать и исследовать алгоритмы формализации. Обработка слабо формализованной информации может быть осуществлена следующим образом. Если поступающая информация представляет собой очень маленькое число событий (одно или несколько), то обработка такой информации – существенная проблема (проблема очень малых выборок), поскольку объяснений единичному событию или нескольким событиям может быть дано много. Если поступающая информация представляет собой небольшое число событий (несколько десятков), то обработка такой информации – существенная проблема (проблема малых выборок), для обработки

которой в некоторых специальных случаях разработаны специальные алгоритмы. Если поступающая информация представляет собой много событий (несколько сотен и более), то для обработки такой информации можно применить статистическую обработку, которая в настоящее время хорошо развита. Если объем поступающей информации большой, то для его обработки требуется много времени. С целью сокращения времени обработки информации предлагается алгоритм, который позволяет распараллеливать обработку информации с помощью кластера высокопроизводительных параллельных вычислений.

Алгоритм обработки слабо формализованной информации включает следующие этапы:

1. Сбор информации;
2. Распознавание информации;
3. Классификация информации;
4. Свертка информации по классам;
5. Оценивание достоверности информации в каждом из классов;
6. Оценивание безопасности информации в каждом из классов;
7. Установление связей между информацией, хранящейся в базе данных, и вновь поступившей;
8. Оценивание вероятности, с которой можно доверять поступающей информации;
9. Поддержка принятия решений в каждом из классов;
10. Обобщенная поддержка принятия решений;
11. Сравнение принятого решения с решениями принятыми раньше;
12. Сохранение принятого решения для последующего использования;
13. Генерация решений;
14. Генерация новой информации.

Этапы, на которых можно распараллелить алгоритм – 1, 4, 5, 6, 7, 8, 9.

На этапе «1. Сбор информации» можно информацию собирать параллельно, если она поступает от различных источников (датчиков).

После этапа «3. Классификация информации» информация обрабатывается в каждом из n классов независимо от других классов и, поэтому, ее обработку можно распараллелить на n потоков (этапы 4–9).

В качестве примера рассмотрено применение алгоритма к обработке генома человека. Таким образом, построен параллельный алгоритм обработки слабо формализованной информации, который может быть реализован на кластере высокопроизводительных параллельных вычислений. Алгоритм включает сбор информации, распознавание информации, классификацию информации, свертку информации, оценивание достоверности и безопасности информации, установление связей между различными видами информации, оценивание вероятности, с которой можно доверять поступающей информации, поддержку принятия решений, сравнение принятого решения с решениями принятыми раньше, генерацию новой информации. В процессе работы алгоритма можно получить совокупность новых геномов, возможно не существующих в природе, которые будут свидетельствовать о наличии каких-либо конкретных заболеваний (или возможности заболеваний). Наличие такой информации позволит облегчить диагностику заболеваний.

Копыльцов А.В., Коршунов К.А., Лукьянов Г.Н., Серов И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Фонд «АЙРЭС», Университет ИТМО

РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СО СТРУКТУРИРОВАННОЙ ПОВЕРХНОСТЬЮ

Рассмотрены проблемы взаимодействия электромагнитного излучения с определенным образом структурированными пластинками (резонаторами «АЙРЭС»). Пластинка представляет собой тонкую кремневую, текстолитовую или сделанную из другого материала пластинку, на которой нанесен рисунок методом травления и представляет собой окружности (щели) образованные прямоугольными канавками глубиной и шириной около 1 мкм. Рисунок подчиняется законам самоподобия и масштабной инвариантности и выполнен на основе аффинных преобразований. Диаметр и толщина пластинки, ширина и глубина канавок могут быть любыми. Электромагнитное поле при взаимодействии с полупроводником вызывает явление смещения зарядов и, вследствие того, что в области щелей пластинка имеет меньшую толщину, концентрация носителей заряда в них выше, чем в соседних областях. Предполагается, что если плотность зарядов в двух соседних щелях велика, то при достижении потенциалом некоторого критического значения возникает пробой по кратчайшему расстоянию между канавками. Излучение падает на пластинку и за счет образования в пластинке свободных электронов, дифракции в щелях и зеркального отражения, в окружающем пространстве образуется преобразованное ‘электромагнитное излучение, которое существенно отличается от падающего на пластинку. Построена математическая модель взаимодействия электромагнитного излучения с пластинкой, на которой нанесен рисунок определенным образом.

Моделировалось как распределение электрических зарядов в пластинке с учетом ее рельефа, так и напряженность электрического поля над ее поверхностью. Учет при моделировании подвижности свободных электронов в пластинке, дифракции в щелях и зеркального отражения от пластинки позволил получить в окружающем пространстве распределение напряженности электрического поля, которое периодически изменяется с течением времени. Математическая модель представляет собой систему дифференциальных уравнений в частных производных, учитывающих дифракцию в щелях, законы отражения от пластинки и законы сохранения для свободных электронов и дырок в пластинке, которые образуются при облучении. Решая эту систему уравнений численными методами, при соответствующих начальных и граничных условиях, можно найти распределения концентрации электронов в пластинке и напряженность электрического поля в пространстве окружающем пластинку. Расчеты проводились на кластере высокопроизводительных параллельных вычислений при различных начальных и граничных условиях, в частности, предполагалось, что сток отсутствует по краям и в центре пластинки. Расчеты показали, что результирующее излучение существенно отличается от падающего, в частности, оно обладает фрактальным самоподобием и над центральной частью пластинки образуется мощная волна излучения, характеристики которой в несколько раз превосходят характеристики падающего излучения. Это можно объяснить тем, что рисунок на поверхности пластинки представляет собой совокупность окружностей расположенных симметрично относительно центра пластинки и тем, что материал пластинки подобран таким образом, что собственная частота колебаний свободных электронов на пластинке и частота падающего излучения близки по величине. Над другими частями пластинки напряженность электрического поля существенно ниже, что может быть использовано, например, для защиты от электромагнитного излучения исходящего от таких приборов, как мобильные телефоны, СВЧ – печи, холодильники и др.

Кузнецов В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

РАСПАРАЛЛЕЛИВАНИЕ ВЫЧИСЛЕНИЙ НА ГРАФИЧЕСКИХ ВИДЕОКАРТАХ

В настоящее время, как при решении прикладных задач, так и задач научно-исследовательской направленности, возникает острая потребность в использовании высокопроизводительных компьютеров. Несмотря на то, что наблюдается тенденция постоянного роста их вычислительной мощности, а также совершенствования IP-сетевых технологий и коммуникационного оборудования, производительности часто не хватает для получения результатов в рамках требуемых временных границ. Поэтому, единственным возможным выходом из этой ситуации является создание более эффективных алгоритмов и технологий по обработке больших массивов данных. В этой области одним из наиболее актуальных и перспективных направлений является распараллеливание вычислительного процесса, организация которого представляет собой важную самостоятельную проблему, что обуславливает наличие множества подходов для её реализации.

Среди прочих, относительно новым, но многообещающим является технология использования ресурсов графических видеокарт для решения задач общего назначения GPGPU (англ. General-purpose graphics processing units - GPU общего назначения). Опыт показывает, что GPU значительно эффективнее CPU при параллельной обработке больших объёмов информации. Это обуславливается тем, что в отличие от центрального процессора, применяемого для вычислений общего характера, узконаправленность развития видеоадаптеров сформировало их особую архитектуру, ориентированную на максимально эффективную обработку графики. Подобные задачи характеризуются выполнением однотипных действий на множественном объёме данных, поэтому GPU реализует модель SIMD (Single Instruction, Multiple Data — одиночный поток команд, множественный поток данных), нацеленную на использование наибольшего количества параллельных потоков, исчисляемых несколькими тысячами, при проведении расчётов.

Основные отличия работы видеоускорителей, в сравнении с CPU, касаются функционирования конвейера выполнения команд, структуры потоков и их обработке, а также многоуровневой системе встроенной оперативной памяти, пропускная способность которой значительно выше оперативной памяти, используемой CPU. В этой связи, производительность центрального процессора и видеокарт при решении определённого спектра задач будет различна. Например, CPU намного эффективнее выполняет расчёты связанные с множественными переходами и ветвлениями. В свою очередь, GPU отлично справляется с массовым параллелизмом и не должен применяться к последовательным алгоритмам. Немаловажным для достижения максимальной эффективности GPGPU вычислений также являются оптимальная работа с памятью устройства и правильная организация потоков для выполнения.

Появление технологии GPGPU позволило не только крупным компаниям, разработчикам, а также специалистам, занимающимся научными исследованиями, существенно повысить производительность вычислений за счёт ресурсов видеокарт. Эта технология уже нашла своё применения в сферах: вычислительных экспериментов на математических моделях, анализе данных, автоматизации проектирования электронных устройств (eda), компьютерной оптики, вычислительной химии и биологии, физике и др.

Применительно к задачам восстановления секретных ключей в защищённых каналах корпоративных сетей, были выполнены вычислительные эксперименты и получены количественные оценки производительности параллельной реализации алгоритма их решения на различных аппаратных средствах. В целом можно отметить, что выигрыш по времени при использовании видеокарт для вычислений может достигать значения в 500 раз по сравнению с CPU. Учитывая тот факт, что в настоящее время персональный компьютер может иметь в комплекте до 7 видеокарт, эффективность их применения для параллельных вычислений не вызывает сомнений.

Ныркov А.П., Воеводский К.С., Князева К.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ ПРИ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЁННОМ ХАРАКТЕРЕ ПРЕДПРИЯТИЯ

В современном мире информатизация и автоматизация процессов затронули подавляющее большинство предприятий, независимо от их масштаба и рода деятельности. Сложно представить условную Почту России без средств автоматизации. Если какое-то конкретное отделение Почты ещё могло бы работать на полностью ручном труде, при этом испытывая огромные трудности в связи с объёмом и загруженностью, то представить, чтобы во всей Почте не было средств автоматизации, просто невозможно.

Рассмотрим абстрактную компанию из торговой сферы или из сферы обслуживания населения. В самом начале жизни компании обычно есть офис и одна точка продаж, штат состоит из 5-10 сотрудников. При подобной схеме строения компании это зачастую физически смежные помещения и объединены в единую компьютерную сеть. Учёт ведётся в электронных таблицах Excel, документооборот внутри компании и с контрагентами - бумажный. Через какое-то время работы компании появляется возможность расширения компании и добавляется ещё одна точка продаж, расположенная в другом месте (городе, регионе, стране) и ещё 5-10 сотрудников. Бумажный документооборот между новой точкой и офисом неоправдан и нерентабелен, потому в употребление внутри компании вводится электронная почта. Часто, даже при наличии сайта, компании используют бесплатные публичные почтовые сервисы (mail.ru; gmail.com; yandex.ru, и т.д.). Одна из мер безопасности, предпринимаемая на данном этапе развития компании – использование собственного почтового сервера. При дальнейшем развитии компании (увеличении количества точек) обычно рассматривается вопрос о внедрении в компании какой-либо автоматизированной системы управления предприятием (далее – АСУП) для автоматизации процессов, защищённого документооборота и моментального контроля бизнес-процессов.

Программный сервер АСУП конфигурируется на выделенном сервере внутри офиса. Взаимодействие удалённых точек с данным сервером происходит посредством канала Интернет. Используется собственное шифрование трафика, либо конфигурируется VPN-канал и точка подключается к общей сети предприятия. Такая АСУП становится основой работоспособности рассматриваемой компании. Обеспечение постоянной бесперебойной работы АСУП и доступа к ней становится ключевой задачей. Для обеспечения надёжности работы производится дублирование каналов связи. Так как у рядового предприятия нет средств и необходимости для прокладки собственных каналов связи, используются существующие каналы интернет-провайдеров. Однако, в случае серьёзного сбоя в электропитании или на магистрали связи отрезанная от внешнего мира часть компании оказывается полностью неработоспособной.

Для исключения таких рисков следует установить на точках отдельные сервера АСУП, а центральный сервер перенести из офиса в частное облако и предусмотреть такую возможность работы локальных серверов, при которой для основных сценариев работы не требуется подключение к центральному серверу. Это позволит точкам несколько часов или даже дней работать автономно, и только потом проводить синхронизацию. Реализация такого сценария работы серверной и клиент-серверной частей АСУП позволит обеспечить максимально успешную и бесперебойную работу компании. Также предложенная схема работы обеспечивает для АСУП три основных свойства информационной безопасности: конфиденциальность, целостность, доступность. Конфиденциальность гарантируется посредством организации защищённых каналов связи и правильного разграничения доступа. Целостность обеспечивается за счёт наличия центрального сервера. Доступность обеспечивается за счёт резервирования каналов связи и использования в Системе собственных серверов на Точках с синхронизацией с центральным сервером. Данные три свойства являются ключевыми, но при комплексном подходе к обеспечению информационной безопасности важно учесть следующие два: аутентичность и апеллируемость. Аутентичность – однозначное установление авторства действий с информацией. В компании подразумевается достаточно большое количество сотрудников и потому необходимо организовать журналирование действий с информацией. Апеллируемость – невозможность отказа пользователя от факта совершения действий с информацией. Оптимальным способом обеспечения апеллируемости является использование неквалифицированной электронной подписи.

Рассмотренная в рамках данной статьи схема построения it-инфраструктуры сетевой компании является универсальной. С использованием данных рекомендаций можно построить практически любое предприятие с территориально распределённой структурой.

Уздяев М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ CUDA В ЗАДАЧАХ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ЛИЦ

В настоящее время распознавание лиц является одной из наиболее важных и актуальных задач в приложениях анализа изображений и компьютерного зрения. Преимущество систем распознавания лиц заключается в том, что они позволяют производить идентификацию личности на расстоянии, без непосредственного участия человека. Такие системы не требуют специальных действий со стороны распознаваемого человека и не ограничивают человека в свободе перемещений.

Одними из наиболее эффективных методов распознавания лиц являются методы, основанные на проекции исходного изображения лица, представленного яркостными признаками в новое пространство, представленное спектральными признаками характеристик изменчивости всех изображений, входящих в обучающую выборку. Целью данных методов является уменьшение размерности исходного пространства признаков (РПП), которое приводит к сокращению вычислительных затрат на этапе распознавания. Данные методы к тому же позволяют преодолеть многие факторы изменчивости изображений лиц и предоставляют высокий уровень корректного распознавания.

Редукция РПП реализуется с помощью представления исходного набора признаков в новом подпространстве и выборе в нем только тех признаков, которые существенно определяют динамику характеристик исходных изображений (например, их энергию).

Методы редукции РПП используют информацию о вариативности исходных данных. Реализуются они в два этапа:

1. Анализ исходных данных на основе метода главных компонент либо на основе линейного дискриминантного анализа. В результате анализа данных определяется матрица проекции, которая наименьшим количеством компонент позволяет представить исходные данные в новом пространстве признаков.

2. Этап ортогонального преобразования в собственном базисе – преобразования Карунена-Лоэва, реализующего проекцию исходных данных в новое пространство признаков и редукцию РПП.

Впервые методы проекции, примененные для обработки изображений, рассматривали их в векторном представлении на основе конкатенации строк или столбцов в общий вектор. В этом случае, для успешного решения задачи распознавания лиц должно выполняться условие: размерность каждого изображения должна быть меньше числа обрабатываемых изображений. При невыполнении данного условия возникает проблема малой выборки.

Изображения, однако, являются двумерными объектами. Учитывая характер изображений, были разработаны методы двумерной проекции. В этом случае каждое обрабатываемое изображение представляется как совокупность векторов-строк и векторов-столбцов. По каждой из совокупности на основе анализа главных компонент либо линейного дискриминантного анализа формируется две матрицы проекции – относительно строк и относительно столбцов. Проекция исходных данных в редуцированное пространство признаков реализуется с помощью двумерного (относительно строк и относительно столбцов изображения) преобразования Карунена-Лоэва.

Данные методы позволяют успешно разрешить проблему малой выборки.

Системы распознавания лиц должны выполнять быструю обработку изображений. Однако, из-за сложной структуры и большой размерности изображения лица требуются большие вычислительные затраты для выполнения быстрой обработки изображения и реализации быстрого распознавания. С целью повышения производительности вычислений и ускорения обработки изображений лиц в системах распознавания необходимо сокращать время обработки при помощи распараллеливания вычислений. В последнее десятилетие значительное развитие получило вычисление на графических устройствах общего назначения, как одно из наиболее перспективных направлений в параллельных вычислениях.

Графический процессор общего назначения является вычислительным устройством с параллельной архитектурой SIMD (Single Instruction – Multiple Data) с общей памятью, реализующим параллелизм на уровне данных.

Для того, чтобы максимально реализовать потенциал вычислений на графических процессорах, необходимо использовать алгоритмы, специально разработанные с учетом принципа параллелизма данных.

В основе методов двумерного анализа главных компонент и метода двумерного линейного дискриминантного анализа лежат следующие матрично-векторные операции: матричное сложение, матричное умножение, инверсия матриц, вычисление собственных чисел и собственных векторов.

Выполнение операций такого вида на графических процессорах позволяет достичь существенного ускорения вычислений относительно вычислений с использованием центральных процессоров, повышая таким образом производительность систем распознавания лиц.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ»

Игнатьев М.Б., Попов В.П., Аксенов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРОБЛЕМЫ СОЗДАНИЯ УМНЫХ АВТОМОБИЛЕЙ И ДОРОГ

В дорожно-транспортных инцидентах гибнет множество людей, что заставляет повышать уровень автоматизации транспортных систем. В докладе рассматриваются проблемы создания умных автомобилей и умных дорог как взаимосвязанных систем. Первая проблема связана с анализом Правил дорожного движения и превращения их в систему паттернов, понятных роботу. Вторая проблема заключается в понимании дорожной ситуации и выработке управляющих воздействий на подсистемы автомобиля, что должно быть осуществлено очень быстро- менее чем за 0,1 секунды. Третья проблема связана с созданием информационно-вычислительной системы автомобиля применительно либо к старой конструкции автомобиля, либо к новой, ка это осуществлено в разработках фирмы GOOGL. Четвертая проблема связана с созданием умной дороги и сети умных дорог, при этом главным требованием к ним является предупреждение участников движения о появлении автомобиля –нарушителя. Пятая проблема связана с системой диагностики автомобиля и водителя, чтобы они в неисправном состоянии не смогли выехать на дорогу, в противном случае к ним может быть применено внешнее управление. Шестая проблема связана с обеспечением оперативной локальной связи между участниками движения, чтобы они в режиме самоорганизации могли обеспечить безопасность движения. Седьмая проблема связана обеспечением ориентации автомобиля на дороге и его навигации на электронной карте. Решение этих проблем осуществляется в рамках молодежного системного проекта и опирается на взаимодействие с автомобильными и компьютерными фирмами.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

АРТОНИКА И МОДЕЛИРОВАНИЕ ДРАМАТИЧЕСКИХ ПРОИЗВЕДЕНИЙ

Артоника – научное направление, связанное с использованием методов и структур искусства в программировании и информационных технологиях на различных уровнях. В искусстве сложился многовековый опыт эффективного воздействия на человека через литературу, музыку, живопись, скульптуру, архитектуру, театр и кино, и представляется целесообразным использовать этот опыт в информационных технологиях. С другой стороны все эти виды искусства пытаются эффективно использовать информационные технологии. Уже сейчас все информационные технологии пронизаны искусством, самые массовые применения ИКТ, миллиардными тиражами, связаны с искусствами и играми. Термин «артоника» был введен Б.Ф.Егоровым, М.Б.Игнатьевым и Ю.М.Лотманом в начале семидесятых годов в рамках тартуских семинаров по семиотике. С тех пор артоника энергично развивается через компьютерные игры, архитектуру виртуальных миров, лингво-комбинаторное моделирование и кибернетическую герменевтику и др. Лингво-комбинаторное моделирование может быть использовано для анализа и синтеза драматических произведений. В качестве ключевых слов можно взять перечень действующих лиц. Например, в пьесе В.Альфьери «Брут» действующие лица – Цезарь, Антоний, Цицерон, Брут, Кассий, Кимвр, Народ, Сенаторы, Заговорщики, Ликторы. Действие происходит в Риме в храме Согласия. Таким образом имеем 10 ключевых слов и лингвистическое уравнение этой пьесы будет

A1*E1 + A2*E2 + …+ A10*E10 = 0

где A1 – характеристика Цезаря, E1 – изменение этой характеристики и т.д. В структуре эквивалентных уравнений будет содержаться 45 произвольных коэффициентов, которые можно использовать для управления действующими лицами, во-первых, при моделировании спектакля и репетициях, во-вторых, для реального управления аватарами – актерами.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

МИР КАК МОДЕЛЬ ВНУТРИ МИРОВОГО СУПЕРКОМПЬЮТЕРА

Как только в конце 40-вых годов прошлого века появилась электронная вычислительная машина, компьютер, так сразу же родилась аналогия между окружающим нас миром и компьютером, и эта аналогия продолжает развиваться и привлекаться для объяснения мироустройства (работы К. Цузе, Э. Фредкина, С. Ллойда и др.). Появление интернета вещей активизировало эти работы (М.Б.Игнатьев «Мир как модель внутри мирового суперкомпьютера»/ Доклад на семинаре Научного совета РАН по методологии искусственного интеллекта в Москве 30 июня 2016 г.). Интернет вещей предполагает наличие связи с различными предметами, вещами, объектами. Следует заметить что и до этого связь с различными объектами поддерживалась людьми с помощью зрения, слуха и механического взаимодействия, но интернет вещей предполагает установление новой дополнительной связи с помощью различных технических средств, что позволит вещам взаимодействовать на новом уровне не только с людьми, но и вещам между собой. Далее, каждый из объектов описывается с помощью лингвистических, математических и компьютерных моделей. Например, солнечная система является специализированным вычислительным устройством для решения задачи многих тел. В итоге вкладывается следующая картина.

Во-первых, компьютеры – системы со структурированной неопределенностью, у них имеется память, которая может быть пустой или заполненной различными данными и программами. Доказано, что универсальные цифровые вычислительные машины могут решать самые разные задачи.

Во-вторых, описание мироустройства на естественном языке, который является универсальной знаковой системой, с помощью лингво-комбинаторного моделирования, превращается в систему уравнений с произвольными коэффициентами, которые и есть структурированная неопределенность. На использовании естественного языка основан и краудсортинг – выявление мнений умной толпы.

В-третьих, архитектура компьютеров непрерывно развивается – эволюционируют элементная база, уровень знаний компьютера, развиваются операционная среда и интерфейсы общения, системы ввода-вывода информации, системы контроля, диагностики и коррекции, системы передачи информации и энергии. Мир заполнен осцилляторами различных типов – это и атомы и молекулы, это и солнечная система и галактики , и все эти осцилляторы включены в общую моделирующую вычислительную систему.

В-четвертых, компьютеры являются вместилищем различных виртуальных миров, которые отделены друг от друга системами защиты информации. Наш мир – это виртуальная ячейка в мировом суперкомпьютере, который является неоднородной распределенной структурой, везде проникающей. В-пятых, компьютеры и сети являются основой самоорганизации социума. Складывается сетевой гибридный интеллект на фоне развития интернета вещей на основе первобытного мышления. Наш современный опыт в своей совокупности составляется из относительно небольшого числа данных и бесконечного числа индукций. Опыт первобытного мышления, напротив, содержит индукции лишь в очень малой пропорции, но зато включает в себя много непосредственных данных, которым мы отказываем в объективной ценности, хотя они, на взгляд первобытного человека, тоже реальны и даже более реальны, чем данные внешних чувств.

Все это позволяет выдвинуть гипотезу о том, что компьютер можно рассматривать как базовую модель самоорганизации Вселенной.

При таком подходе становится понятным, почему нам до сих пор не удалось установить связь с инопланетянами. Ведь если наш мир не более чем модель внутри мирового суперкомпьютера, то для того, чтобы установить такую связь необходимо изучить структуру мирового суперкомпьютера, его аппаратного и программного обеспечения, изучить систему защиты между мирами, и вот тогда, может быть, удастся установить связь с обитателями других миров. Вторжение инопланетян возможно через киберпространство. Это колоссальная фундаментальная задача для современной науки.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

СЕТЕЦЕНТРИЧЕСКИЕ СИСТЕМЫ УПРАВЛЕНИЯ

Системы моделирования поля боя (МПБ) являются основой так называемых сетецентрических систем управления войсками. 23 июня 2009 г. министр обороны США Роберт Гейтс подписал приказ о создании кибернетического командования – структуры, ответственной за безопасность военных информационных сетей. Американская концепция «сетецентрической войны» подразумевает превращение вооруженных сил США в единый гигантский разведывательно-ударный комплекс, где все связаны со всеми линиями передачи информации и находятся в едином информационном пространстве. Это позволит постоянно отслеживать оперативную обстановку и немедленно

принимать решения. Но в этой системе не решены задачи оптимального соотношения самоорганизации и внешнего управления.

Суть сетецентрического управления заключается в том, чтобы формировать приказы управления войсками с учетом взаимодействия всех родов войск и всех данных разведки о противнике. Например, для управления четырьмя боевыми платформами составляется первое лингвистическое уравнение

A1*E1 + A2*E2 + A3*E3 + A4*E4 = 0,

где A1 – характеристика боевой платформы 1, E1 – приказ об изменении характеристики платформы 1, A2 –характеристика боевой платформы 2, E2 – приказ об изменении характеристики платформы 2, и т.д. и структура эквивалентных уравнений будет иметь вид

E1 = U1*A2 + U2*A3 + U3*A4

E2 = - U1*A1 + U4*A3 + U5*A4

E3 = - U2*A1 – U4*A2 + U6*A4

E4 = - U3*A1 – U5*A2 – U6*A3

откуда очевидно, что каждый приказ формируется с учетом характеристик всех других платформ и подстраивается с помощью произвольных коэффициентов. Если известна информация о противнике в виде второго лингвистического уравнения

B1*E1 + B2*E2 + B3*E3 + B4*E4 = 0,

то структура эквивалентных уравнений будет иметь вид

E1 = U1*D123 + U2*D124 + U3*D134

E2 = - U1*D213 – U2*D214 + U4*D234

E3 = U1*D312 – U3*D314 – U4*D324

E4 = U2*D412 + U3*D413 + U4*D423

где D23 = A2*B3 – A3*B2 и т.д. , B1- характеристика боевой платформы противника, противостоящей платформе A1, B2 – характеристика боевой платформы противника, противостоящей платформе A2 и т.д. В этом случаем приказы E1,…,E4 будут вырабатываться с учетом сил противника, а для подстройки используются четыре произвольных коэффициента.

Попов В.П.
Россия,Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ДОСТОИНСТВА И НЕДОСТАТКИ УЖЕ ПОСТРОЕННЫХ УМНЫХ АВТОМОБИЛЕЙ. ОПЫТ ЭКСПЛУАТАЦИИ

Многие автомобильные фирмы Санкт-Петербургского кластера уже внедряют отдельные функции в автомобили, которые продаются, и уже накоплен опыт их эксплуатации.

Бортовые мультимедийные системы управления автомобилем, присутствующие на рынке и уже повсеместно доступные на некоторых марках автомобилей, по своим функциям достаточно полезные:

– Традиционные системы контроля, диагностики и обслуживания автомобиля, вместе с системой контроля давления в шинах, сиденья с памятью, удержания отката при трогании на подъёмах и др.

– Системы помощи водителю и системы автономного вождения:

1) система ограничения и управления скоростью;
2) активная система помощи при парковке;
3) система информации на участках при плохой обзорности (мёртвые зоны види-димости;
4) система распознавания дорожных знаков;
5) система предупреждения столкновений;
6) система управления режимов работы подвески и адаптивного рулевого управления;
7) система круиз-контроля;
8) элементы iphone-телефонии и голосового (речевого) управления;
9) система управления микроклиматом;
10) система адаптивного управления и переключения переднего света фар;
11) система помощи и удержания полосы движения;
12) система динамической стабилизации;
13) аудиосистема и др.

Наряду с полезными и оправданными сервисными функциями, некоторые из них кажутся избыточными и оставляют впечатление “чего бы ещё такое придумать“, или требуют доработок, необходимость в которых проявилась в процессе эксплуатации автомобиля.

Например:

– лампочки для порогов в зеркалах заднего вида;
– фоновая подсветка пространства в салоне с возможностью выбора желаемого цвета;

– многие функции перешли от кнопок к многоуровнему меню (всплывающим окнам с несколькими уровнями погружения), в частности, управление распределением потоков нагретого воздуха и многие другие. Выбор пунктов меню производится во время движения автомобиля, и в условиях интенсивного движения с большой скоростью, это может потребовать съезда на обочину;

– задающий команду через систему речевого распознавания иногда получает неадекватную реакцию. В лучшем случае автомобиль сообщает, что вас не понимает, а в худшем пытается сделать что-то свое (часто, это проявляется при работе с нави-гатором);

– датчик дождя: пара капель на лобовом стекле (стекло практически сухое), но он уже включает дворники и они “молотят” сухое лобовое стекло, причем с увеличением скорости (прибавлением газа) скорость дворников возрастает.

– если мало информации с боковых зеркал можно заказать подключение телевизионной камеры заднего вида при движении на дисплей. Если она при движении не загрязняется, то это удобно. Но у многих автомобилей TV-камера находится в зоне, куда попадает грязь из под колёс, и эффект от TV-камеры снижается.

– электрический стояночный тормоз – не сильно освобождает место в салоне по сравнению с нормальным “ручником“ , но в критической ситуации воспользоваться таким тормозом (не глядя) вряд ли получится.

– усилитель руля с переменным передаточным отношением: на невысоких скоростях руль “острый“, а с ростом скорости руль “тупеет“. В принципе к этому можно привыкнуть, но переменное передаточное отношение заставляет водителя напрягаться.

Таким образом, идея умного автомобиля уже превратилась в реальность и продолжает развиваться.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Абакумов А.А.
Россия, Санкт-Петербург, Университет ИТМО

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДИК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В настоящее время все большую популярность набирает аудит информационной безопасности. Одним из популярных направлений аудита информационной безопасности является тестирование на проникновение с использованием методик социальной инженерии. Данный метод подразумевает большое количество подготовительных работ: разработка управляющего сервера, создание полезной нагрузки, системы мониторинга и др. Однако, на данный момент не существует открытого инструментария, позволяющего относительно просто и в короткие сроки реализовать такое тестирование.

В данной работе представлена разработка программного комплекса для проведения тестирования на проникновения с использованием методик социальной инженерии операционных систем семейства «Windows». Комплекс разработан с нуля с использованием таких языков программирования как Golang и Javascript, и использует набор базовых функций интерфейсов WINAPI. Кроме этого реализована идея обратного DNS туннеля, который позволяет установить связь с управляющим сервером, в случае недоступности его по HTTP протоколу. Данный комплекс позволяет специалисту по информационной безопасности в кратчайшие сроки спланировать и реализовать необходимые компоненты для проведения тестирования; провести пост-эксплуатацию для подтверждения факта успешной атаки и закрепления на тестируемой системе; составить сводную статистику по результатам выполненных работ.

Гатауллин Р.И.
Россия, Санкт-Петербург, Университет ИТМО

АНАЛИЗ ВОЗМОЖНОГО ПОВЕДЕНИЯ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУЛЬТИАГЕНТНОЙ СИСТЕМЕ ПРИ ИСПОЛЬЗОВАНИИ АЛГОРИТМОВ ФЛОКИРОВАНИЯ

При использовании мультиагентных систем (МАС) в задачах, связанных с обеспечением информационной безопасности, возможно подразделение всех агентов на классы в зависимости от того, какая цель должна быть выполнена тем или иным агентом. К таким классам относятся неинформированные и информированные агенты, а также агенты-диверсанты. Задача каждого агента состоит в достижении определённой цели; неинформированные агенты изначально не имеют цели, последние два типа агентов имеют собственную цель (соответственно истинную и ложную). Для нормального функционирования МАС важно снизить влияние на неё нарушителей. Успешное противодействие нарушителям реализуемо с помощью проведения анализа их поведения в мультиагентной среде.

Для анализа взаимодействия компонентов МАС используется симулятор, позволяющий проводить различные эксперименты на основе полученных входных данных о количестве агентов различного типа, их местонахождению, свойствах и расстоянию относительно друг друга. В качестве алгоритма, описывающего взаимодействие агентов с точки зрения их передвижения, реализован т.н. boids - алгоритм группового перемещения, в основе которого лежат такие принципы, как сплочённость, разделение и выравнивание скоростей. Благодаря реализации этих принципов в симуляторе МАС агенты, причисляющие себя к одной группе, стараются держаться рядом, не сталкиваясь между собой и передвигаясь с одной скоростью.

В симуляторе реализовано поведение обычных и т.н. «умных» нарушителей. Обычные нарушители начинают движение к своей цели с самого начала симуляции, вектор их направления сразу направлен в сторону ложной цели. «Умные» нарушители изначально ведут себя подобно неинформированным агентам и активизируются при достижении т.н. «дистанции саботажа». При активации вектор направления диверсанта плавно изменяется с каждым шагом от истинной цели по направлению к ложной. В ходе экспериментов было замечено, что эта модель поведения нарушителей является наиболее эффективной – даже сравнительно малое число диверсантов в группе способно увести за собой весь рой, поставив нормальное функционирование МАС под угрозу.

Исходя из этого ставится вывод о необходимости проведения анализа поведения таких нарушителей в МАС с целью нахождения возможных путей уменьшения их влияния на неинформированных агентов.

Данные по анализу собираются с помощью симулятора, который позволяет проводить опыты с изменением всех основных параметров (в том числе и случайным), а также сохранять результаты по каждому опыту в текстовом виде. Сбор данных возможно производить автоматически.

На данном этапе исследований предпочтительным методом анализа является регрессионный анализ – метод, позволяющий определить, какие из параметров опыта наиболее сильно влияют на конечные результаты (главным из которых является число агентов, дошедших до «истинной» цели). Также планируется проведение кластерного анализа с целью классификации данных и определения наборов входных данных – опытов, при воспроизведении которых функциональность МАС будет наиболее защищена.

По итогам проведения анализа планируется определить степень воздействия «умных» агентов-диверсантов на МАС по сравнению с обычными, неинформированными агентами, а также разработать способы нейтрализации их воздействия на рой.

Дикий Д.И., Рожкова Е.О., Артемьева В.Д., Савченко-Новопавловская С.Д.
Россия, Санкт-Петербург, Университет ИТМО

КЛИЕНТ-СЕРВЕРНОЕ ПРИЛОЖЕНИЕ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ПОЧЕРКУ

Согласно, данным аналитического центра InfoWatch за первое полугодие 2016 года, 90% утечек были связаны с компрометацией персональных данных. За этот период были скомпрометированы более 262 миллионов записей, в том числе платежная информация, обладание которой может привести к явным финансовым потерям. Поэтому следует уделять огромное внимание угрозам, свойственным удаленному несанкционированному доступу.

Для того чтобы реализовать атаку на информационную систему, злоумышленник должен получить доступ к ней. Наиболее защищенные системы предполагают физический доступ в определенное помещение в определенное время. Однако на практике такие системы не распространены. Наоборот, большой популярностью пользуются сервисы, предполагающие удаленный доступ к каким-либо услугам. Такие системы более подвержены атакам подмены легального пользователя. Именно усовершенствование защиты таких информационных систем будет рассматриваться в работе.

С давних пор, человек использовал свою рукописную подпись в качестве доказательства того, что именно он совершил некое действие, например при подписании договора. И действительно, сравнивая два образца подписи, можно с некоторой уверенностью сказать были ли они сделаны одним и тем же человеком. Однако, кроме обычного сравнения изображения подписей, в качестве уникальной характеристики человека можно использовать их динамические характеристики, проявляющиеся в процессе написания. Именно динамические характеристики подписи человека будут рассматриваться как подтверждение легальности пользователя.

Цель работы состоит в разработке и исследовании программного обеспечения производящего операцию аутентификации пользователя по динамическим характеристикам его почерка, реализуемую через общедоступные телекоммуникационные сети, в частности сеть Интернет.

Для достижения поставленной цели были сформированы конкретизирующие условия, определяющие параметры применения разрабатываемого программного обеспечения. Предполагается, что у пользователя и злоумышленника имеется необходимое программно-аппаратное устройство ввода, в частности графический планшет. Вторым немаловажным условием является использование браузеров для подключения информационной системе. Другими словами, определена возможность прохождения легальности с любого места, где есть выход в сеть Интернет без необходимости установки какого-либо вспомогательного десктопного приложения.

Предметом исследования работы являются алгоритмы и структуры программного обеспечения, применяемые в системах аутентификации по динамическим характеристикам почерка, их производительность и эффективность.

Результаты, изложенные в работе, могут быть использованы для решения задачи модернизации, улучшения процесса аутентификации по динамическим характеристикам рукописного почерка, где это необходимо.

Реализация программной части выполнена в среде разработки IntelliJ IDEA на языке программирования Java и представляет собой одно серверное приложение, построенное в виде сервлетов. Система функционирует на операционных системах серверов, где предустановлена Java Virtual Machine. Кроме основного приложения используются написанный на языке программирования javascript вспомогательный скрипт, функционирующий со стороны клиента, который легко можно адаптировать под уже настроенные информационные системы.

Разработанный программно-аппаратный комплекс аутентификации пользователя по динамическим характеристикам почерка представляет собой полностью готовый к использованию программный продукт, обладает оптимальными характеристиками и требованиями к функционированию, полностью выполняет возложенные на нее задачи, имеет в распоряжении весь необходимый набор возможностей.

Зайцева Н.М.
Россия, Санкт-Петербург, Университет ИТМО

КОЛИЧЕСТВЕННАЯ ОЦЕНКА ПОТЕРЬ ОТ ПРАВОНАРУШЕНИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ

На сегодняшний день информационная среда является очень привлекательной сферой деятельности для правонарушителей. Особенностью правонарушений в информационной сфере является то, что существенный вред можно нанести внезапно, минимальными силами и средствами.

При расследовании правонарушения в первую очередь необходимо определить характер и размер причиненного вреда или ущерба. В случае с материальными объектами ущерб можно определить на основании стоимости замены или восстановления. Оценить ущерб от нарушения свойств нематериального объекта, такого как информационный актив, гораздо сложнее.

Проанализировав исследования в данной области, можно сделать вывод, что только количественная оценка величины ущерба позволяет определить реальные последствия от совершенного правонарушения.

С точки зрения защиты информации наиболее важны три свойства информации: конфиденциальность, целостность и доступность. Исходя из этого, убытки от правонарушения предлагается оценивать как совокупность ущерба, причиненного вследствие нарушения каждого из этих свойств.

Нарушение конфиденциальности возникает в случае разглашения информации неуполномоченным лицам. В этом случае потери складываются из нескольких составляющих: затраты на оповещение пострадавших, расследование утечки, оплату юридических услуг в случае судебных разбирательств. Возможна выплата штрафов и затраты на проведение PR-кампании для восстановления репутации.

Целостность информации нарушается путем преднамеренного или случайного искажения данных. Непреднамеренное изменение представляет собой сбои, отказы системы и т.д. Преднамеренное – умышленное изменение с целью получения выгоды, и представляет больший для нас интерес.

Убытки от нарушения целостности включают в себя:

- потери от модификации информации;
- потери, связанные с восстановлением информации;
- потери, связанные с утратой возможного дохода.

Нарушение доступности информации подразумевает частичное или полное ограничение доступа к ресурсу. Потери от угроз доступности рассчитываются как совокупность потерь от несвоевременного оказания услуг по доступу к информации, убытков, связанных с восстановлением информации с упущенной выгодой. Также учитываются потери, связанные с простоем деятельности.

При оценке ущерба необходимо учитывать как финансовые потери, так и нематериальные потери. Используя описанный выше подход, можно оценить убытки от различных правонарушений в информационной среде.

Золотарева Е.Н., Золотарева К.Н.
Россия, Санкт-Петербург, Университет ИТМО

КРИМИНАЛИСТИЧЕКАЯ ИДЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИОННЫЙ ПРИЗНАК В КИБЕРПРЕСТУПЛЕНИЯХ

Криминалистическая идентификация один из основных методов установления истины в уголовном судопроизводстве, когда возникает необходимость выявить связь подозреваемого, принадлежащих ему предметов и других объектов с расследуемым событием по оставленным следам и иным материальным отображениям. Суть идентификации заключается в том, чтобы по отображениям установить конкретный объект, который их оставил. Поэтому с криминалистической точки зрения характеристику компьютерного преступника целесообразнее считать понятием собирательным в широком смысле этого слова, хотя и с некоторым делением на самостоятельные обособленные группы по ряду оснований.

Безусловно, специфика совершения компьютерных преступлений связана с фактическим отсутствием межгосударственных границ. Но УК РФ предусмотрен ряд наказаний за киберпреступления, так как правовой защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее владельцу, пользователю и иному лицу. Именно поэтому подчеркивается общественная опасность каких-либо действий с вредоносными программами и не только.

Таким образом, мы рассмотрели 4 направления, по которым можно идентифицировать преступника с точки зрения криминалистики. К ним относятся:

- Определение преступного поведения: подразумевает собой мотивацию преступника, что побудило его к действиям, здесь можно выделить три основных направления нарушения – это личный интерес, корыстные побуждения, конкуренция, в любом случае все направлено на нарушение целостности, конфиденциальности и доступности таким образом, чтобы нанести наибольший ущерб;
- Техническая оснащенность преступника (с использованием или без использования компьютерных средств): в данном случае конечно сложнее искать преступника, если он использует специальные средства, так при их использовании сложнее определить местоположение подозреваемого, так как в информационном пространстве возможна подмена ip-адресов;
- Определение обстановки совершения преступления: здесь особое внимание необходимо уделить профессиональной сфере, так как чаще всего преступления подобного характера встречаются в работе с финансовыми, банковскими информационными технологиями;
- Квалификация преступника: область данного направления достаточно обширна, так как уровень квалификации, может быть какой угодно, начиная от новичка-хакера и заканчивая опытным шпионом.

Помимо направлений, рассмотренных выше важно учитывать социально-психологические условия, как идентификационный признак киберпреступлений, в которых ведется расследование. Настрой общества по отношению к информационным преступлениям под воздействием средств массовой информации периодически меняется. Это обстоятельство влияет на поведение участников расследования. Полярными значениями этих отношений является неприятие действий преступников, совершивших действия, влияющие на интересы некоторых слоев общества в отдельной стране до возвеличивания отдельных преступников.

Однако все эти преступления связаны с нарушением установленного порядка профессиональной деятельности и личных интересов. Становится понятно, что для правонарушителей в данной области обычно ясен механизм нарушения правил пользования информационными ресурсами и его связь с событиями, повлекшими наступление криминального результата.

Таким образом, можно сказать, что проблемы в данной области обусловлены отчасти отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов. Кроме того, с появлением нового средства обработки информации компьютер и программное обеспечение могут быть предметом законных и незаконных сделок, а также предметом хищения как ценных объектов или противоправного использования. Они могут быть также инструментом преступной деятельности, например, средствами незаконного доступа к удаленным информационным ресурсам, инструментами разработки и запуска «компьютерных вирусов», причиняющих существенный материальный ущерб, хранилищем и инструментом обработки информации о преступной деятельности, например, данных о действительном состоянии учета и движения материальных ценностей, о партнерах по противоправным сделкам и их содержании, использованы как средство подготовки управленческих решений, которые повлекли негативные результаты.

Иоффе М.А., Нурдинов Р.А.
Россия, Санкт-Петербург, Университет ИТМО

ПОВЫШЕНИЕ ТОЧНОСТИ И ОБЪЕКТИВНОСТИ ОЦЕНКИ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ БЕЗОПАСНОСТИ

Распространенность качественной оценки рисков связана с тем, что количественная оценка вероятности реализации угрозы весьма затруднена ввиду отсутствия четких требований к составу исходных данных, правил оценки (математической модели) и достаточного количества статистических данных.

Однако сама по себе качественная оценка рисков не позволяет аргументировать размер инвестиций в безопасность, так как не содержит конкретных цифр для определения затрат в случае реализации угроз, а значит и аргументировать стоимость работ, направленных на снижение рисков. Для определения экономической эффективности использования мер и средств защиты информации интерес представляет количественная оценка риска.

Основные проблемы на сегодняшний день заключаются в низкой точности и субъективности результатов оценки вероятности, а также в неопределённости правил учета данных об инцидентах ИБ при прогнозировании вероятности.

Таким образом, целью работы стало повышение точности и объективности определения вероятности реализации угрозы за счет использования данных об инцидентах информационной безопасности.

Также в работе предложена методика динамического обучения предложенной модели. Процесс обучения заключается в корректировке весовых коэффициентов метрик на основании данных о реализованных или предотвращенных угрозах с применением метода обратного распространения ошибки в последовательном режиме.

Применение метода обратного распространения ошибки для аппроксимации функции вероятности реализации угрозы обусловлено рядом преимуществ, среди которых стоит выделить нетребовательность к входным данным и возможность исключения из модели незначимых и добавления новых метрик в процессе обучения.

Проведен ряд экспериментов, подтверждающих достоверность и результативность предлагаемых модели и методики её обучения.

Преимущества предложенного метода:

- высокая точность результатов оценки (при выборке из 100 инцидентов средняя ошибка менее 3%, при выборке из 1000 инцидентов – менее 1%);
- высокая гибкость (возможность обучения не неполных данных);
- возможность реагирования на изменения области оценки за счет динамического обучения в последовательном режиме;
- значительное сокращение роли и объема работы экспертов.

Из преимуществ разработанного модуля следует выделить то, что его использование позволяет существенно сократить роль и объём работы экспертов при оценке рисков и, прежде всего, вероятности реализации угроз, а также возможность осуществлять динамическую переоценку и обучение при изменении входных данных и, таким образом, оперативно реагировать на изменения окружающей среды.

Канев А.Н., Настека А.В., Бессонова Е.Е.
Россия, Санкт-Петербург, Университет ИТМО

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ СИСТЕМЫ «УМНЫЙ ДОМ»

В настоящее время быстро развиваются системы «Умный дом» (УД). УД – системы управления зданием, позволяющие контролировать все подсистемы здания. На такие системы возложены функции по обеспечению безопасности здания, оптимизация происходящих в нем процессов, управление оборудованием и др. От верного исполнения данных функций зависит сохранность личного имущества (в т.ч. безопасность сведений), безопасность здания, а также жизнь людей.

Нередко УД строится с применением беспроводных сенсорных сетей (БСС). БСС – беспроводная распределенная самоорганизующаяся сеть датчиков, исполняющих устройств и устройств управления. Их использование обусловлено такими свойствами БСС, как масштабируемость, низкое энергопотребление и малые габариты. Но при этом БСС подвержены сетевым атакам, что показано в ряде существующих работ.

Таким образом, необходима система защиты БСС УД. С этой целью предлагается выявлять аномалии БСС с применением методов машинного обучения.

Цель работы – разработка механизма выявления аномалий в БСС УД.

Для достижения поставленной цели авторы решают ряд задач:

- анализ существующих характеристик устройств БСС УД, определение характеристик для выявления аномалий;
- анализ и тестирование методов машинного обучения в программной модели, сравнение результатов тестирования и выбор оптимального метода;
- тестирование механизма выявления аномалий на физических устройствах.

На данный момент среди характеристик, позволяющих отслеживать аномальные воздействия, были выделены следующие:

- количество входящих/исходящих пакетов за единицу времени;
- количество потерянных пакетов/ошибок за единицу времени;
- мощность исходящего сигнала;
- потребление электроэнергии за единицу времени.

Среди методов машинного обучения авторами выделены следующие:

- логистическая регрессия;
- метод опорных векторов;
- метод ближайшего соседа;
- стохастический линейный спуск;
- наивный байесовский классификатор;

- деревья решений;
- некоторые модели искусственной нейронной сети.

Для тестирования методов используются два самостоятельных модуля. Первый модуль представляет собой БСС в среде моделирования Omnet++, выполняющей сценарий активности БСС УД. Данные о значениях характеристиках устройств БСС из первого модуля поступают во второй. Второй модуль является программной реализацией метода машинного обучения, которая на основе данных значений характеристик формирует отчет о найденных аномалиях.

В дальнейшем авторами работы планируется тестирование механизма выявления аномалий на физических устройствах. В ходе него должна быть произведена оценка эффективности механизма выявления аномалий.

Предлагаемый механизм предполагается использовать в целях раннего выявления атак или неполадок работы БСС УД.

Кривцова И.Е., Салахутдинова К.И.
Россия, Санкт-Петербург, Университе ИТМО

УСЛОВИЯ ПРИМЕНЕНИЯ КРИТЕРИЯ ПИРСОНА ДЛЯ ИДЕНТИФИКАЦИИ ИСПОЛНЯЕМЫХ ФАЙЛОВ

В данной работе под идентификацией следует понимать процесс распознавания некоторого файла как отождествление его с той или иной программой. В настоящее время существуют различные методы по идентификации файлов, но большинство из них исходят из определения целостности, например, побайтовое сравнение, сравнение контрольной суммы или цифровой подписи. Все эти методы не применимы к таким исполняемым файлам как elf, в силу их открытости, что приводит к постоянным модификациям и созданиям новых версий таких файлов.

Объектом исследования в настоящей работе являются способы идентификации исполняемых файлов; предметом исследования – ограничения критерия Пирсона при идентификации файлов. Цель исследования – выявление проблем использования критерия и формулировка условий его применения.

В качестве меры отличия двух, построенных по разработанному ранее методу, сигнатур исполняемых файлов был выбран статистический критерий Пирсона. Он прост в понимании и использовании, однако ограничения данного критерия, такие как: объем выборки, частота встречаемости признака для каждого разряда интервала значений частот, одинаковость разрядов для сравниваемых распределений, порождают некоторые проблемы его использования. Так, объединение наблюдаемых данных в группы связано с потерей информативности о функции распределения первоначальных данных; возникает необходимость сравнивать различные по длине интервалы значений частот исследуемых признаков elf-файлов; возникает необходимость подбирать эмпирически уровни значимости критерия ввиду того, что один и тот же признак имеет различные длины распределений в разных версиях программ.

Перед исследователем возникает ряд задач, которые необходимо решить для того, чтобы данный статистический критерий использовался корректно. Такими задачами могут быть: поиск информативного признака; выбор способа подсчета частот признака; обработка файлов как малого, так и большого объемов и т.д.

Решение описанных задач возможно при выполнении следующих условий:

- предварительное использование методов по оценке информативности признаков исполняемых файлов;
- формирование одинаковых длин интервалов значений частот, но различных для файлов различного объема;
- дополнительное использование других методов исследования, например, линейной аппроксимации.

Коржук В.М., Демяшев А.Н.
Россия, Санкт-Петербург, Университет ИТМО

ПРОБЛЕМА УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Ввиду широкого применения беспроводных сенсорных сетей на критически важных объектах, к безопасности сетей и передаваемых по ним данным могут предъявляться особенно строгие требования. В отличие от классических компьютерных систем, наиболее серьезный класс угроз для сенсорных сетей исходит от скомпрометированных узлов, поэтому алгоритмы, обеспечивающие работу сети, должны быть адаптированы к динамически изменяющейся структуре сети, быть устойчивыми к захвату, блокированию или неправильному поведению определенного количества узлов (в процентном соотношении).

Одной важнейших проблем криптографии беспроводных сенсорных сетей (WSN - wireless sensor network) является проблема управления ключами (KMS – Key Management System), в частности, задача безопасного распределения ключей. Это является следствием описанных выше

особенностей WSN, главным образом, подверженности сенсоров физическому воздействию и ограниченности их вычислительных ресурсов.

Большинство современных протоколов, на основе которых работают WSN (например, широко распространенный ZigBee, Z-Wave и др.), основано на стандарте IEEE 802.15.4, определяющем физический слой и управление доступом к среде. Этот стандарт, хотя и предусматривает использование ключей для обеспечения конфиденциальности передаваемых данных, не уточняет способов безопасного распределения ключей. За последние годы появилось большое количество протоколов управления ключами, все они имеют свои преимущества и недостатки (сравнительную характеристику основных протоколов можно найти в работе).

Требования к системе управления ключами в WSN можно разделить на два класса: требования безопасности и эксплуатационные требования.

В разделе Требования безопасности WSN перечислены основные требования к WSN, среди которых наиболее важными для KMS являются устойчивость и самоорганизация. Хотя конфиденциальность, целостность и актуальность данных также важны, существующие сегодня криптографические решения могут быть применены для WSN (с небольшими изменениями). С другой стороны, учитывая специфику организации сенсорных сетей, требованию самоорганизации оказывается труднее удовлетворить. Так, сенсорные узлы должны быть способны установить новые соединения в районе вышедшего из строя узла, но это требование может быть нарушено, если узлы будут неспособны устанавливать новые соединения без нужных ключей. Требованию устойчивости также нелегко удовлетворить. Узлы WSN часто находятся в неконтролируемой зоне и подвержены физическому воздействию, в т. ч. захват и как следствие полный контроль атакующего над узлом.

В класс эксплуатационных требований к системе управления ключами входят требования, отражающие эффективность системы. Так как KMS, не удовлетворяющие требованиям безопасности, не должны быть использованы, сравнение систем происходит по критериям основных эксплуатационных требований:

1. Доступность служебной информации системы управления ключами. Промежуточные узлы сети должны обеспечивать надежную передачу сообщений за приемлемое время. Доступность KMS зависит от способности узлов к обмену сообщений, однако и сама система не должна сильно нагружать сеть. KMS должна быть организована с учетом топологии сети и типа передачи данных;

2. Гибкость системы управления ключами определяется устойчивостью системы при изменении топологии сети, а также возможностью добавления новых и исключения скомпрометированных узлов;

3. Масштабируемость системы управления ключами определяется устойчивостью системы при увеличении размера сети. Сети, работающие по стандарту IEEE 802.15.4, теоретически способны поддерживать до 65,536 узлов. Система управления ключами должна быть способна обслуживать все узлы сети.

Лейфер К.И.
Россия, Санкт-Петербург, Университет ИТМО

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО БИОМЕТРИЧЕСКИМ ХАРАКТЕРИСТИКАМ ЖЕСТОВ НА СЕНСОРНОМ ЭКРАНЕ

В наши дни смартфоны, оснащённые сенсорными дисплеями, получили повсеместное распространение. Сенсорный экран в смартфонах – довольно точное и отзывчивое устройство ввода. В большинстве современных смартфонов тачскрин способен распознавать до 10 одновременных касаний с точностью до пикселя, считывать около 50 событий ввода в секунду, а так же позволяет определять площадь каждого из касаний. Это позволяет отслеживать с высокой точностью каждый жест пользователя, оставляемый им на сенсорном экране. Можно предположить, что жесты, вводимые пользователем на сенсорном экране, могут обладать неким набором уникальных для каждого человека особенностей, то есть содержать в себе набор некоторых биометрических признаков. Сенсорный экран, исходя из перечисленных выше особенностей, вполне способен зафиксировать эти признаки, выступая в роли биометрического сенсора. В рамках работы было реализовано клиент-серверное приложение. Клиентская часть устанавливается на устройства тестовых пользователей и отслеживает все жесты, вводимые ими на сенсорном экране. Эта часть собирает необходимую статистику и затем автоматически отправляет собранные данные на сервер. Серверная часть проекта сохраняет всю статистику в базе данных. Клиентская часть представляет собой android-приложение, которое устанавливается на смартфоны с включенным полным доступом к устройству. Серверная часть написана на языке JavaScript с использованием платформы Node.js. В течение двух недель от 19 тестовых пользователей получено примерно 200000 событий ввода. Для нахождения характеристик событий ввода, обеспечивающих наибольшую вероятность успешной идентификации пользователя, необходимо провести анализ собранных данных. С этой целью построена и протестирована тестовая система идентификации, работающая по следующему принципу: 1. Для каждого пользователя производится выборка определённого количества событий ввода. Строится распределение этой выборки по исследуемой характеристике. Полученное

распределение является эталонным вектором для каждого пользователя. 2. Оставшиеся события ввода для каждого пользователя разбивается на выборки определённого размера и строится их распределение по той же характеристике. Полученные распределения являются тестовыми векторами. 3. Для каждого тестового вектора вычисляется наиболее близкий эталон по расстоянию Евклида. Идентификация считается успешной, если тестовый и эталонный векторы принадлежат одному пользователю.

Мурадов А.Р., Викснин И.И.
Россия, Санкт-Петербург, Университет ИТМО

ПРИМЕНЕНИЕ И АДАПТАЦИЯ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ АНАЛИЗА ПОВЕДЕНИЯ ТОЛПЫ В УСЛОВИЯХ ОГРАНИЧЕННЫХ ПРОСТРАНСТВ

В условиях ограниченного пространства поведение больших скоплений людей может быть сложно предсказуемым, а также опасным для человеческих жизней, находящихся в условиях давки и экстремальных ситуациях.

Для минимизации ущерба человеческому здоровью в помещениях с ограниченным пространством и ограниченным количеством выходов возможно проведение мер по прогнозированию потенциального ущерба с помощью различных инструментов моделирования.

Была разработана модель поведения толпы в условиях эвакуации из помещения с ограниченным пространством. Модель разрабатывалась в среде моделирования AnyLogic. В рамках модели были разработаны несколько типов агентов и угроз, которые возможно применить к любому замкнутому пространству:

1. Агенты
- Позитивные агенты – обычные люди в условиях экстремальной ситуации
- Негативные агенты – люди, которые увеличивают ущерб позитивным агентам и агентам-персонала.
- Агенты-персонала – люди, помогающие обычным позитивным агентам уменьшить ущерб в условиях экстремальной ситуации

2. Угрозы
- Террористический акт
- Взрыв
- Пожар
- Перестрелка
- Давка в условиях ограниченного пространства и малого количества выходов.

Разработанные алгоритмы были протестированы на двух реальных ситуациях для того, чтобы проанализировать достоверность разработанной модели в целом и отладить работу системы:

3. Пожар в клубе «Хромая Лошадь» 5 декабря 2009 года в Перми.

4. Террористический акт в аэропорту Стамбула имени Ататюрка 29 июня 2016 года.

Также, в процессе разработки модели был разработан алгоритм взаимодействия агентов в условиях давки для дальнейшего анализа помещений на предмет опасных зон.

Полученные результаты показали, что разработанные алгоритмы и модель в целом может быть использована для анализа помещений с ограниченным пространством на предмет угрозы жизни в условиях экстремальной ситуации, когда жизни десятка или сотни людей может зависеть от правильного подхода к планировке помещения.

Назыров М.В., Викснин И.И.
Россия, Санкт-Петербург, Университет ИТМО

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ РАБОТЫ МОДЕЛИ ДВИЖЕНИЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Информационная безопасность подразумевает обеспечение доступности, конфиденциальности и целостности информации. В работе рассматривается один из аспектов информационной безопасности мультагентных систем (МАС) – целостность информации.

Целостность информации МАС – возможность любого агента системы получить истинную информацию о другом агенте и его действиях согласно установленным ограничениям взаимодействия в рамках рассматриваемой системы. При выполнении данного правила каждый агент сможет иметь представление не только о своих действиях и об окружающем его участке среды, но и в целом об окружающей среде и состоянии роя.

Применение механизмов доверия и репутации позволяет контролировать адекватность получаемой от других участников роя информации. При этом остается вероятность умышленного или неумышленного появления в группировке роботов-диверсантов. Несмотря на достаточно хорошие результаты функционирования модели доверия и репутации, возникает ряд ситуаций, когда поставленные перед роем цели либо не выполнены, либо выполнены не в полном объеме. Таким образом, диверсанты выполняют свою основную задачу – снижают работоспособность роя.

Для решения проблемы появления диверсантов требуется классифицировать нарушителей и определить основные алгоритмы их работы. Исходя из принципов работы роя, можно определить следующие основные виды диверсантов:

1) обычные нарушители;
2) нарушители, которые анализируют положение других роботов;
3) сломавшиеся роботы;
4) диверсанты, сообщающие ложное расстояние до цели;
5) диверсанты, передвигающиеся в некорректном направлении;
6) диверсанты, выдающие себя за легитимных агентов.

Ниже представлено пошаговое описание деятельности роботов.

– Шаг I – формирование вектора оценок эффективности, обмен информацией об оценках между всеми участниками роя; формирование матрицы D, содержащей сведения о расстоянии до цели.

– Шаг II – проверка данных массива D с помощью встроенной аппаратуры; формирование матрицы V, содержащей данные о достоверности полученных данных (т.е. элемент матрицы будет равен «1», если данные достоверны, «-1» – в противном случае; значение «0» элемент принимает в случае нахождения робота вне зоны видимости).

– Шаг III – вычисление репутации агентов (на основе оценок, полученных от других агентов), формирование массива оценок агентов S и общего вектора оценок Q.

– Шаг IV – учёт изменения уровня репутации с течением времени: скалярное умножение вектора Q на величину F(l), где F(l) – функция Вейбулла-Гнеденко.

– Шаг V – вычисление вспомогательных векторов H, G, P, L, формирование итогового вектора уровня доверия W, определяющее роль агента в системе, опознанную роем.

– Отдельно рассматривается дополнительный шаг, в ходе которого происходит распределение роботов по целям и осуществление движения по направлению к ним.

Стоит отметить, что шаг I выполняется некорректно для всех типов нарушителей, кроме типа «диверсанты, передвигающиеся в некорректном направлении» (у данного типа в массив D записываются случайные значения расстояний до целей).

Патрикеев Р.О., Щепин Н.Д.
Россия, Санкт-Петербург, Университет ИТМО

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ БОЛЬШИХ СКОПЛЕНИЙ ЛЮДЕЙ В УСЛОВИЯХ РАЗЛИЧНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

В связи с тем, что модель поведения человека в группе отличается от модели поведения человека вне группы, возникла потребность анализа последствий различных информационных воздействий на поведение группы.

Используя графическую среду для имитационного моделирования «Anylogic», было разработано несколько моделей для различных ситуаций, в которых принимали участие различные типы агентов(людей):

– Обычные агенты (рядовые члены группы, ведут себя как обычные люди).

– Позитивные агенты (противоборствуют негативным агентам).

– Негативные агенты (пытаются различными способами увеличить ущерб, нанесенный позитивным и обычным агентам).

Целью исследования является минимизация ущерба, полученного позитивными и обычными агентами (в данном контексте, ущерб представляет собой урон, полученный людьми) при возникновении чрезвычайной ситуации.

Всего для моделирования было выбрано 2 инцидента, наглядно демонстрирующих поведение групп людей в различных условиях:

Пожар в клубе «Хромая лошадь», Россия, г. Пермь, 5 декабря 2009 года. Погибло 111 человек. Еще 45 скончалось в больницах в последующие дни.

Теракт в международном аэропорту имени Кемаля Ататюрка. Турция, г. Стамбул, 28 июня 2016 года. Погибло 42 человека, 239 получили ранения.

В ходе проведения исследования, чтобы достичь соответствия в ущербе, полученном людьми при реальных обстоятельствах и ущербе, полученном агентами в смоделированной ситуации была использована базовая модель поведения пешеходов, описанная в «Pedestrian Library» среды «Anylogic». На данную модель были наложены различные дополнительные механизмы воздействия агентов между собой и воздействия агентов с окружающей средой. Благодаря нововведениям обычные агенты смогли следовать за позитивными, обходить огонь, убегать из зоны покрытия взрыва и выбирать оптимальный для себя путь эвакуации. Так же было детально проработано воздействие агентов в случае давки. Используя импульсное взаимодействие удалось максимально приблизить данную модель к реальности.

Затем был разработан ряд мер, способствующий повышению выживаемости обычных и позитивных агентов, в заданных условиях:

- Повышение количества позитивных агентов.
- Понижение количества негативных агентов.
- Изменение размера выходов.
- Изменение количества выходов.
- Незначительные изменения во внутренней архитектуре помещений.

Благодаря данным, полученным в ходе проведения исследования, существует возможность оценки ущерба при возникновении различных чрезвычайных ситуаций, а так же минимизирования последствий данных ситуаций.

Ральникова Н.С.
Россия, Санкт-Петербург, Университет ИТМО

ДАКТИЛОСКОПИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Проблема идентификации человека чаще всего возникает при разграничении доступа к различным объектам и ресурсам. В привычных системах идентифицируется не сам человек, а нечто, им предъявляемое: документ, ключ, карточка, пароль и т. п., каждый из которых может быть подделан, потерян, украден, забыт, передан другому лицу. Такое положение вещей является абсолютно неприемлемым для серьезных систем контроля доступа, а посему встает вопрос об идентификации именно человека, что возможно лишь при применении биометрических систем контроля и управления доступом.

Пальцы человека имеют особый папиллярный рисунок, уникальный для каждого индивидуума. Современные системы контроля доступа, основанные на дактилоскопии, как раз и используют этот рисунок (отпечатки пальцев) в качестве идентификатора. Преимущества данной технологии очевидны: отпечатки пальцев невозможно взломать, весьма сложно скопировать, к тому же полностью исключается вероятность кражи идентификатора (как это часто случается с теми же смарт-картами).

Тем не менее, дактилоскопическая идентификация имеет и свои недостатки. Так, около 4% людей имеет плохое качество отпечатков. Люди, занятые в ручном труде, получают многочисленные мелкие травмы, что создает большие трудности при сравнении отпечатков.

В основе любой системы дактилоскопической идентификации лежит сканер отпечатков пальцев. Это малогабаритный прибор, считывающий изображение отпечатка непосредственно с пальца человека. Вторым важным компонентом является контроллер – электронный модуль, который идентифицирует считанный отпечаток пальца, и принимает решение о допуске.

Для того чтобы человек получил в системе право доступа, он должен быть зарегистрирован в ней как пользователь. Регистрация предполагает ввод в систему отпечатков одного или нескольких пальцев и имени пользователя.

Для получения доступа пользователь прикладывает палец к поверхности сканера, система преобразует графическое изображение его папиллярного рисунка в математический слепок, который сравнит с базой данных всех ранее введенных отпечатков пальцев. В случае совпадения происходит авторизация и контроллер системы передает сигнал на исполнительное устройство - турникет, электромагнитный замок и т.п.

При всем многообразии биометрических систем, возможно упрощенно классифицировать их и разделить их на три типа:

- преобразующие отпечатки пальцев в цифровой код при помощи оптического сенсора;
- преобразующие отпечатки пальцев посредством линейного теплового датчика;
- преобразующие отпечатки пальцев используя ёмкостный датчик.

Дактилоскопические системы позволяют исключить проникновение на объект посторонних лиц, а также четко разграничить охраняемую территорию на зоны ответственности, допуская в определенные места исключительно персонал требуемой квалификации.

Сравнительно же новым направлением использования биометрических систем по отпечатку пальца является эффективный учет рабочего времени. Дело в том, что современные системы контроля доступа позволяют записывать факт идентификации в журнал событий, в последующем формируя на его основании подробный отчет о перемещении каждого сотрудника.

Рожкова Е.О., Дикий Д.И.
Россия, Санкт-Петербург, Университет ИТМО

DLP-СИСТЕМА КАК СРЕДСТВО ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Человеческое звено как составляющая часть автоматизированной системы в процессе профессиональной деятельности является слабо защищенным, так как человеку свойственны ограничения и ошибки. При работе с критичными данными непреднамеренные ошибки могут нанести

ощутимый, зачастую непоправимый ущерб. Так, внося в систему ложные данные, оператор будет считать их верными. Особенно острой эта проблема становится в условиях дефицита времени, в экстремальных ситуациях. Кроме того, получая распоряжения по корректировке данных от вышестоящего руководства, человек-оператор, как правило, не сомневается в подлинности таковых. Здесь срабатывает определенная психологическая установка: никто не хочет приобрести неприятности, споря с начальством. Таким образом, поскольку системы управления различными предприятиями составляют основу эффективной деятельности компании, то вмешиваясь в циркулирующий информационный поток, направляя его в то или иное, выгодное злоумышленнику, русло можно нанести значительный ущерб предприятию в целом, подорвать его репутацию и пошатнуть лидирующие позиции.

В современных условиях наиболее эффективным является принцип «контролируй», нежели «защищай». Действительно, существует возможность полностью ограничить круг общения сотрудников одной компании в рабочее время исключительно корпоративными ресурсами. Однако, нет уверенности в том, что в свободное время они не будут обмениваться конфиденциальной информацией. Как выяснить, ведется ли корпоративная переписка только с держателями разрешенных почтовых ящиков, или используются посторонние ресурсы? Что послужило причиной ошибки, которую совершил человек, до этого зарекомендовавший себя как профессионально мотивированный оператор? Как раз на эти вопросы и отвечает DLP-система. Она является идеальным инструментом в проведении служебных расследований. Позволяет контролировать пути, по которым возможно распространение информационно-психологического воздействия на человека. Так, человек, не обладая специфическими знаниями и навыками о DLP-системе, может не знать, что на его компьютере установлено данное программное обеспечение. Проверка действий администраторов нередко обусловливает ключевой аспект в контроле над системой в целом.

Комплекс используемых решений должен разрабатываться исходя из нужд и политики информационной безопасности конкретной компании. При этом требуется соблюдать баланс между эффективной и не затрачивающей множества ресурсов системы и максимально удовлетворяющем нужды компании контролем над информационными потоками, курсирующими внутри корпоративной сети и выходящими за её пределы.

Важно подчеркнуть, что с каждым годом методы воздействия на пользователя, в том числе методы социальной инженерии становятся все изощреннее. Однако, невзирая на предпринимаемые руководителями предприятий меры, злоумышленники проводят успешные атаки и применяют направленное информационно-психологическое воздействие, заставляя оператора совершать действия, противоречащие корпоративной политике безопасности, совершенно осознанно. При этом жертва зачастую даже не подозревает, что своими незначительными относительно масштабов предприятия действиями открывает канал утечки информации. Чтобы этого избежать, требуется создавать комплекс мер и мероприятий по поддержанию уровня информационной безопасности предприятия на должном уровне.

Спивак А.И., Спивак О.И., Шидакова Д.Н.
Россия, Санкт-Петербург, Университет ИТМО

УГРОЗЫ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ

Накопление, хранение и последующая обработка данных, собираемых в больших количествах различными системами становится неотъемлемой частью практически любой информационной системы. Рост объемов данных дает толчок к использованию новых перспективных технологий для их хранения. Последующая обработка дает необходимые исходные данные для построения рекомендательных систем, систем принятия решения и прогнозирования событий. Многие из современных систем хранения предоставляют возможности для распределенной обработки.

Вследствие большой значимости в составе информационной системы (ИС) функции хранения данных к ней предъявляются даже большие требования по обеспечению безопасности работы, чем к другим компонентам ИС. Важность выделения, систематизации и оценки угроз безопасности, существующих в распределенных системах хранения данных, обусловлено центрального местом в структурной схеме построения ИС. Анализ угроз безопасности позволяет сформировать количественные показатели функционирования таких систем, отражающие уровень их защищенности от всех типов деструктивных воздействий.

Распределенные системы хранения на текущем этапе развития не представляются однородными по используемым стекам технологий. По особенностям функционирования их можно разделить на 4 типа, каждый из которых обладает своим собственным перечнем актуальных угроз безопасности.

Наряду с принципами хранения можно выделить степень организованности данных, подлежащих хранению: неструктурированные, слабоструктурированные, структурированных, гибридные. В зависимости от типа данных в системе различаются как способы манипулирования с ними, так и технологии обеспечения безопасности при доступе к данным. Одновременно с этим

системы, сочетающие работу с разными по степени организованности типами данных, значительно усложняют анализ угроз безопасности вследствие нелинейных эффектов взаимного влияния механизмов обработки данных.

Наиболее изученными со стороны исследователей являются распределенные реляционные базы данных, которые обладают развитым набором средств обеспечения безопасности данных, которые включают в себя средства разграничения доступа, криптографическую защиту данных, технологии защищенного сетевого взаимодействия, аутентификация субъектов доступа. Ко второму типу систем распределенного хранения относятся NoSQL нереляционные базы данных, которые работают со слабоструктурированными данными. Угрозы безопасности, возникающие при использовании такого вида БД прежде всего доступность и целостность, вследствие неполного соответствия теореме CAP.

Системы наподобие Apache Hadoop относятся к системам хранения неструктурированных данных, которые обладают высокой способностью к горизонтальному масштабированию без относительно к структуре хранимых данных. Встроенные механизмы репликации данных не полностью отвечают требованиям обеспечения целостности данных, вследствие отсутствия влияния со стороны среды, в которой осуществляется хранение. Доступность получения данных в сложных средах со множественным доступом к отдельным узлам хранения также не учитывается в политике распределения данных по узлам.

Системы хранения данных «в памяти» являются наиболее перспективным направлением развития систем распределенного хранения данных. Ввиду особенности хранения данных в памяти дополнительно к стандартным к данному виду систем угрозам целостности и доступности, связанным с распределенным характером системы, добавляется необходимость гарантированной синхронизации данных с энергонезависимым источником.

Для построения модели угроз, которая может быть использована для управления безопасностью систем хранения, возможно выделение количественные показателей к стандартным видам угроз безопасности распределенных систем хранения.

Авторами выделяются два крупных типа угроз: целостности и доступности. В качестве основных показателей для первого типа угроз являются время, достаточное для перераспределения данных для подержания уровня реплицирования всех данных системы при выходе из строя узлов.

Количественные показатели доступности позволяют оценить максимальную, среднюю и минимальную скорость доставки данных до клиента при всех режимах работы системы, включая аварийный.

Данные показатели являются одними из многих оказывающие влияние на оценку работы распределенной системы хранения.

Выделенные в рамках исследования угрозы безопасности для нескольких типов систем хранения, а также формирование требований по оценки доступности и целостности дает возможность количественной оценки систем хранения по уровню безопасности.

Чалыкин И.Г.
Россия, Санкт-Петербург, Университет ИТМО

РАЗРАБОТКА СКАНЕРА УЯЗВИМОСТЕЙ СУБД ORACLE RDBMS

Oracle Database или Oracle RDBMS — это объектно-реляционная система управления базами данных компании Oracle. Многие годы является наиболее популярной СУБД. К сожалению, даже самые последние версии этой базы данных с актуальными исправлениями нельзя назвать абсолютно защищенными. Еще больше уязвимостей появляется ввиду неправильного внедрения данной СУБД или её некорректной настройки. Впрочем, подобные ошибки можно выявить с помощью специализированных сканеров.

На данный момент на рынке присутствует немало специализированных программных комплексов для автоматизированного сканирования с целью определения уязвимостей. Существуют подобные утилиты и для СУБД Oracle RDBMS. Типовой сканер уязвимостей определяет факт наличия определенной уязвимости по сигнатуре или по версии приложения называет ее критичность в зависимости от заранее заложенных метрик. В подобном, классическом, подходе сканер на выходе выдает плоский список обнаруженных уязвимостей.

Целью данной работы является попытка оптимизировать процесс автоматизированной диагностики слабостей и уязвимостей.

Для этого предлагается использовать следующие понятия:

– База знаний. По факту, является экземпляром небольшой базы данных, куда записывается вся обнаруженная при сканировании техническая информация - логины пользователей, пути установки Oracle RDBMS, имена процеду и т.д. В дальнейшем, использование этих данных может качественно улучшить последующие проверки.

– Алгоритм “конечный автомат”. Использование данного алгоритма в качестве основной архитектуры сканера позволит проводить диагностику более тщательно, поскольку процесс сканирования не ограничивается количеством сигнатур.

В данном докладе планируется рассмотреть подробно данные решения, их особенности, преимущества, отличия от уже существующих решений и возможные технические пути реализации.

Цветков Л.В.
Россия, Санкт-Петербург, Университет ИТМО

ИСПОЛЬЗОВАНИЕ МОДЕЛИ ПРОГРАММНОГО КОДА ДЛЯ ОБНАРУЖЕНИЯ ПРОГРАММНЫХ ДЕФЕКТОВ

Причиной появления различного рода уязвимостей в программных продуктах является наличие в них ошибок или дефектов. Причины возникновения дефектов различны: ошибка разработчика, невнимательность, неполная логическая проработанность, нескоординированная эволюция частей системы. Чем раньше будет обнаружен внесенный дефект, тем меньше будут затраты на его устранение. Поэтому необходимо производить поиск внутри первичного источника ошибки – в исходном коде программы. Составляя модель программы, необходимо не только корректно представить в ней зафиксированный в исходном коде порядок выполнения, но и обеспечить семантичность модели. Данному требованию удовлетворяет подход, основанный на синтезе системы зависимой типизации и формы статического единственного присваивания (SSA). Благодаря наличию в зависимом типе информации о ограничениях на использование в виде абстрактной переменной, возможно отражение, восстановление и анализ на семантическом уровне различных свойств программы.

Используемая модель позволяет проводить анализ программы на предмет наличия различного рода ошибок, в частности ошибок доступа к памяти и управления ресурсами. В модели учтены такие возможности императивных языков как создание псевдонимов и изменение значения переменных, что позволяет использовать модель непосредственно для анализа таких языков, как C.

Преимуществом используемой модели является возможность восстановления различного рода ограничений на переменные исходя из типичных для переменных данного типа фрагментов графа исполнения. Немаловажно, что для этого не используются дополнительные аннотации исходного кода, что позволяет проводить подобный анализ в автоматическом режиме.

Обнаруженные дефекты непосредственно влияют на защищенность программы от деструктивных входящих воздействий. Одним из результатов анализа, наряду с идентифицирующей дефект информацией является предположения о возможных входных данных, приводящих к неопределенному поведению и нарушению безопасности программы. Основываясь на предложенной информации, разработчик может принять решение о путях исправления обнаруженного дефекта. Таким образом, применение данной модели приводит к повышению защищенности программных продуктов.

ОГЛАВЛЕНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ 17

Советов Б.Я.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ТЕНДЕНЦИИ РАЗВИТИЯ ВЫСШЕГО ОБРАЗОВАНИЯ И ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 17

Соколов Б.В., Юсупов Р.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
НЕОКИБЕРНЕТИКА: НЕОГРАНИЧЕННЫЕ ВОЗМОЖНОСТИ И ВОЗМОЖНЫЕ ОГРАНИЧЕНИЯ 18

Черешкин Д.С., Сичкарук А.В.
Россия, г. Москва, Федеральный исследовательский центр «Информатика и управление» РАН
ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ОБЪЕКТОВ 18

Шевчик А.П., Мусаев А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)
КОГНИТИВИСТИКА: НОВЫЙ ВЫЗОВ ИНФОРМАЦИОННОЙ ЭРЫ 21

Рузанова Н.С., Кудряшова С.В., Никольская Н.В.
Россия, г. Петрозаводск, Петрозаводский государственный университет, Администрация Главы Республики Карелия
СОКРАЩЕНИЕ ЦИФРОВОГО НЕРАВЕНСТВА И ПРЕДОСТАВЛЕНИЕ ЭЛЕКТРОННЫХ УСЛУГ В РЕСПУБЛИКЕ КАРЕЛИЯ 21

Тимофеев Д.А.
Россия, г. Севастополь, Главное управление информатизации и связи г. Севастополя
ОСОБЕННОСТИ РАЗВИТИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В ГОРОДЕ СЕВАСТОПОЛЕ 24

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
КОНСТИТУЦИОННЫЙ ХАРАКТЕР ИНСТИТУТОВ ТАЙН 25

Горбунова И.Б.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МУЗЫКАЛЬНОМ ОБРАЗОВАНИИ 26

Жигадло В.Э.
Россия, Санкт-Петербург, ООО «СимплГрупп»
ОСОБЕННОСТИ РЕАЛИЗАЦИИ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ 27

Микони С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОБЛЕМЫ КАЧЕСТВА РЕЙТИНГОВОГО ОЦЕНИВАНИЯ В УСЛОВИЯХ РЫНОЧНОЙ ЭКОНОМИКИ 28

РЕГИОНАЛЬНАЯ ПОЛИТИКА ИНФОРМАТИЗАЦИИ. ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО 29

Видясова Л.А.
Россия, Санкт-Петербург, Университет ИТМО
БАРЬЕРЫ НА ПУТИ РАЗВИТИЯ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ 29

Гордейчук А.А., Жук Д.В.
Россия, Санкт-Петербург, ООО «Интеллектуальные информационные системы», Университет ИТМО
ВОЗМОЖНОСТИ ТЕХНОЛОГИЙ С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ 29

Горелик С.Л., Лещинский В.В., Иванов И.А., Малахов А.А.
Россия, Санкт-Петербург, Университет ИТМО
г. Москва, Аналитический центр при Правительстве Российской Федерации
ТРЕТЬЕ ПОКОЛЕНИЕ ТЕРРИТОРИАЛЬНЫХ ПАССАЖИРСКИХ ТРАНСПОРТНЫХ СИСТЕМ 30

Григорьев Л.Ю., Кононова О.В.
Россия, Санкт-Петербург, Бизнес инжиниринг групп, Университет ИТМО
МОДЕЛИРОВАНИЕ СИСТЕМ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ НА ОСНОВЕ АРХИТЕКТУРНО-ИНЖЕНЕРНЫЙ ПОДХОДА 31

Зенченкова К.С., Чугунов А.В.
Россия, Санкт-Петербург, Университет ИТМО,
НП «Партнерство для развития информационного общества на Северо - Западе»
СИСТЕМА МОНИТОРИНГА ПОРТАЛОВ ЭЛЕКТРОННОГО УЧАСТИЯ КАК ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО СОПРОВОЖДЕНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВЛАСТИ 32

Дмитрова О.А.
Россия, Санкт-Петербург, Университет ИТМО
ПОДХОД К ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМУ ОБЕСПЕЧЕНИЮ АНТИНАРКОТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА 33

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ МЕГАПОЛИСОМ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА 34

Кондратьев В.В.
Россия, Санкт-Петербург, Университет ИТМО
ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ 34

Коршунов И.Л., Левкин И.М., Микадзе С.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
О СОЗДАНИИ ИССЛЕДОВАТЕЛЬСКОГО РЕГИОНАЛЬНОГО СИТУАЦИОННОГО ЦЕНТРА МОНИТОРИНГА КОНКУРЕНТНОЙ ОБСТАНОВКИ В ИНФОРМАЦИОННОЙ СФЕРЕ 35

Лавреш И.И.
Россия, Республика Коми, г. Сыктывкар, ГАУ РК «Центр информационных технологий
О СТРАТЕГИИ ИМПОРТОЗАМЕЩЕНИЯ В СФЕРЕ ИТ РЕСПУБЛИКИ КОМИ 36

Мисников Ю.Г., Филатова О.Г.
Республика Беларусь, г. Минск,
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный университет
КОНЦЕПЦИЯ СОЗДАНИЯ ИНСТРУМЕНТАРИЯ ОБРАТНОЙ СВЯЗИ ДЛЯ ПОРТАЛА ОБЩЕСТВЕННОЙ ПАЛАТЫ САНКТ-ПЕТЕРБУРГА 37

Скатин А.В.
Россия, Санкт-Петербург, ООО «Консист»
ПЕРИОДЫ РАЗВИТИЯ АВТОМАТИЗАЦИИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ 38

Чугунов А.В.
Россия, Санкт-Петербург, Университет ИТМО
РАЗВИТИЕ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ: ПО МАТЕРИАЛАМ СИСТЕМНОГО ПРОЕКТА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА 39

Шубинский М.И.
Россия, Санкт-Петербург, Университет ИТМО
СОЗДАНИЕ МЕЖРЕГИОНАЛЬНОГО ПИЛОТНОГО РЕСУРСНОГО ЦЕНТРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СЕВЕРО-ЗАПАДЕ РОССИИ 40

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ 42

Балакирев Н.Е.
Россия, г. Москва, Московский авиационный институт (национальный исследовательский университет)
ПОТЕНЦИАЛЬНАЯ СУЩНОСТЬ ПЕРЕДАВАЕМОЙ И ВОСПРИНИМАЕМОЙ ИНФОРМАЦИИ 42

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ИНТЕРНЕТ ВЕЩЕЙ И ГИБРИДНЫЙ ИНТЕЛЛЕКТ 43

Ильина О.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МЕТОДОЛОГИЯ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ И СЕРВИСОВ 43

Касаткин В.В., Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ 45

Морозов С.А
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
РЕАЛИЗАЦИЯ VFS В UNIX ПОДОБНЫХ СИСТЕМАХ 46

Мотиенко А.И., Салухов В.И., Солдатенко Т.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
УПРАВЛЕНИЕ ГЕОЭКОЛОГИЧЕСКИМ РЕЗЕРВОМ ИНФРАСТРУКТУРЫ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА 47

Охтилев М.Ю., Потрясаев С.А., Соколов Б.В
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МЕТОДОЛОГИЯ И ТЕХНОЛОГИЯ КОМПЛЕКСНОГО МОДЕЛИРОВАНИЯ СЛОЖНЫХ ТЕХНИЧЕСКИХ ОБЪЕКТОВ 47

Рыжков С.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ ПЕРИМЕТРА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ..... 48

Салухов В.И., Солдатенко В.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛЬ ИННОВАЦИИ ДЛЯ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ЭКСПЕРТИЗЫ ПРОЕКТА СЕТИ СВЯЗИ..... 48

Свиньин С.Ф., Алексеев А.В., Попов А.И., Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный морской технический университет, Северный (Арктический) федеральный университет имени М.В. Ломоносова
ТЕОРИЯ ИНФОРМАЦИИ: ОТ ТЕОРЕМЫ УИТТЕКЕРА-КОТЕЛЬНИКОВА-ШЕННОНА К ТЕОРИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ..... 49

Терехин Д.В., Климов А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
РОЛЬ И МЕСТО РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ ПРИ ОРГАНИЗАЦИИ КОЛЛЕКТИВНОЙ РАБОТЫ НА СРЕДСТВАХ АВТОМАТИЗАЦИИ 50

Хомоненко А.Д., Халил М.М., Андрук А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
АЛГОРИТМЫ РАСЧЕТА ОПЕРАТИВНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ПОМОЩЬЮ МОДЕЛЕЙ МНОГОКАНАЛЬНЫХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ С «ОХЛАЖДЕНИЕМ» ... 51

Трофимов В.В., Трофимова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
КАТЕГОРИАЛЬНЫЙ АНАЛИЗ ТЕРМИНА «ИНФОРМАЦИЯ»..... 51

Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНТЕЛЛЕКТУАЛИЗАЦИЯ МАШИННОЙ ИМИТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ..... 52

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ 54

Авраменко В.С., Бобрешов-Шишов Д.И., Соловьев В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИДЕНТИФИКАЦИЯ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ 54

Авраменко В.С., Деньжонков К.А., Чирушкин К.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВОЕННО-УЧЕБНОГО ЗАВЕДЕНИЯ 55

Анистратов И.В., Калюка В.И., Морозов Д.А.
Россия, г. Краснодар, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,
Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АЛГОРИТМИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ АНАЛИЗА СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА 55

Апарина Е.Ю., Зубакин В.В.,Сазонов В.В., Титов В.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АВТОМАТИЗАЦИЯ ПЛАНИРОВАНИЯ И ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ПОЛЕВОЙ СИСТЕМЫ ОБМЕНА ДАННЫМИ ТАКТИЧЕСКОГО ЗВЕНА 56

Бакунин С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ ОБМЕНА ДАННЫМИ 57

Башкирцев А.С., Шинкарев С.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПЕРСПЕКТИВНЫЙ ОБЛИК АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СВЯЗЬЮ СИЛОВЫХ МИНИСТЕРСТВ И ВЕДОМСТВ 58

Бегмахмудов И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ПРИКЛАДНОГО ПРОГРАМмНОГО ОБЕСПЕЧЕНИЯ В ХОДЕ ПРОГРАМмНО – ЦЕЛЕВОГО ПЛАНИРОВАНИЯ В СИЛОВЫХ СТРУКТУРАХ 59

Бернардо А.К., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
О ПРОБЛЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ СЛУЧАЙНЫХ ВОЗДЕЙСТВИЙ И АВАРИЙНЫХ СИТУАЦИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 60

Бирюков М.А., Брунилин А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
УПРАВЛЕНИЕ РАЗГРАНИЧЕНИЕМ ДОСТУПА КАК ВАЖНЕЙШАЯ ЗАДАЧА ИНТЕГРАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЕДИНОМ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОМ ПРОСТРАНСТВЕ 60

Богачев К.Г., Мещанин В.Ю.
Россия, Санкт-Петерубург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ СЦИ НА ВНОВЬ ПРОЕКТИРУЕМЫХ СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ: СКРЫТЫЕ ПРЕИМУЩЕСТВА ИЛИ ОШИБКА ВЫБОРА? 61

Болдырев П.А., Яцков А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ АКУСТИЧЕСКОЙ РАЗВЕДКИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ 62

Боровкова М.А., Сидорова А.П., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТКРЫТОМ СЕГМЕНТЕ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ НА ОСНОВЕ КОНТЕНТ-АНАЛИЗА СЕТЕВОГО ТРАФИКА 63

Богаченко Д.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ЧИСЛЕННЫХ МЕТОДОВ ДЛЯ РЕШЕНИЯ ЗАДАЧ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ АНТЕННЫХ СИСТЕМ 63

Богданов А.В., Котяшичев И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
БОРТОВАЯ ШИРОКОПОЛОСНАЯ АНТЕННА С КОМБИНИРОВАННЫМИ НАГРУЗКАМИ ДЛЯ БЛА 64

Бровин Д.Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПОСТРОЕНИЯ ТРАНСПОРТНЫХ СЕТЕЙ ПОЛЕВОЙ ВОЕННОЙ СВЯЗИ 65

Вайчикаускас М.А., Мондикова Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КЛАССИФИКАЦИЯ ПРИНУЖДАЮЩИХ АТАК И СХЕМ ОТРИЦАЕМОГО ШИФРОВАНИЯ..... 65

Ванчугов А.Н., Грибков В.А., Федоров П.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СПОСОБ УПРАВЛЕНИЯ ВХОДНЫМИ ПОТОКАМИ СООБЩЕНИЙ, ИСПОЛЬЗУЮЩИЙ ИНФОРМАЦИЮ О СОСТОЯНИИ СЕТИ И ОБЕСПЕЧИВАЮЩИЙ ЗАЩИТУ ОТ ПЕРЕГРУЗОК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 66

Васюков Д.Ю., Яцков А.В., Болдырев П.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДИКА ВОЕННО-ЭКОНОМИЧЕСКОГО ОБОСНОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 67

Виноградов А.Б., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННЫЙ КОНТРОЛЬ ИЗМЕНЕНИЯ СОСТОЯНИЯ КОНТРОЛИРУЕМОГО ИНФОРМАЦИОННОГО ОБЪЕКТА 68

Винокуров А.В., Махов Д.С.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
РАЗРАБОТКА ПРОГРАММНО-АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ АДАПТИВНОЙ ОБРАБОТКИ ВИДЕОИНФОРМАЦИИ НА БОРТУ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА..... 69

Волков Д.В.
Россия, Санкт-Петербург Военная академия связи имени Маршала Советского Союза С.М. Буденного
МУЛЬТИАГЕНТНЫЙ ПОДХОД К ПОСТРОЕНИЮ ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ СВЯЗИ ОБЩЕВОЙСКОВОГО СОЕДИНЕНИЯ..... 69

Вольхин С.Д., Алашеев В.В., Пустошкин М.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ЗАДАЧИ МОНИТОРИНГА ПОМЕХОВОЙ ОБСТАНОВКИ С ЦЕЛЬЮ ФОРМИРОВАНИЯ ИСХОДНЫХ ДАННЫХ ДЛЯ ОЦЕНКИ ЭЛЕКТРОМАГНИТНОЙ ДОСТУПНОСТИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ 70

Воробьев А.И., Колбанёв А.М., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОДИРОВАНИЕ МАРКЕРОВ НА ПОВЕРХНОСТНЫХ АКУСТИЧЕСКИХ ВОЛНАХ..... 71

Воробьев А.И., Колбанёв А.М., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ И ЕЕ ПРИМЕНЕНИЯ..... 71

Воронков К.Л., Рожнов М.Д., Шерстюк Ю.М
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
АРХИТЕКТУРА СОВРЕМЕННОЙ КОМПЛЕКСНОЙ СИСТЕМЫ МОНИТОРИНГА ИНФОТЕЛЕКОММУНИКАЦИЙ..... 72

Воронков К.Л., Курилов Д.А., Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек Балтика»
УНИФИКАЦИЯ СРЕДСТВ УПРАВЛЕНИЯ СОВРЕМЕННЫМ ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ 73

Вотинов М.Л., Уйманов А.В., Пустошкин М.М., Репников А.Ю.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОЦЕНКА ДОСТУПНОСТИ ДЛЯ НАРУШИТЕЛЯ ЗАЩИЩАЕМЫХ РЕСУРСОВ СИСТЕМЫ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТЬЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 73

Васильева О.Н, Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛЬ ЭЛЕКТРОННОГО КОНСТРУКТОРА ДЛЯ ИЗУЧЕНИЯ СРЕДСТВ СВЯЗИ ПОЛЕВЫХ УЗЛОВ СВЯЗИ 74

Галаган А.О.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИССЛЕДОВАНИЕ ТРЕБОВАНИЙ И МЕТОДОВ ПРОКЛАДКИ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ В ПОЛЕВЫХ УСЛОВИЯХ..... 75

Ганин П.А., Михалев О.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СИНХРОННОЕ ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ И СОСТАВЛЕНИЕ КАРТЫ ПО СТЕРЕОИЗОБРАЖЕНИЮ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ НАВИГАЦИИ В РОБОТОТЕХНИКЕ 76

Горчаков В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИССЛЕДОВАНИЕ ВОПРОСОВ ПОСТРОЕНИЯ СИСТЕМЫ СВЯЗИ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ 77

Данилова Е.И., Зотов Д.Г., Ракицкий С.Н., Ракицкий Д.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДИКА ОЦЕНКИ СВОЕВРЕМЕННОСТИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ 77

Дубенецкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТЬЮ, ОРИЕНТИРОВАННАЯ НА ОБЪЕКТНУЮ МОДЕЛЬ ПРОЦЕССОВ..... 78

Егупов М.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ЭЛЕКТРОННЫХ-ИНФОРМАЦИОННЫХ РЕСУРСОВ 79

Жук А.А., Климов А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПЛАНИРОВАНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ 80

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ТРАНСПОРТОМ В МЕГАПОЛИСЕ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА 81

Жигадло В.Э.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»
ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ МЕГАПОЛИСОМ - «SMART SITY» 81

Журавель Е.П.
Россия, Санкт-Петербург, АО «НИИ «Рубин»
МОДЕЛИ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ 84

Журавель Е.П.
Россия, Санкт-Петербург, АО «НИИ «Рубин»
МОДЕЛИ УСЛУГ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ 85

Журавель Е.П., Журавель П.Н., Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «НИИ «Рубин», АО «РАМЭК-ВС», АО «Институт инфотелекоммуникаций»
МОДЕЛИ ВОЗДЕЙСТВИЙ НА РЕСУРСЫ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ 86

Зайцев Ф.С., Кузнецов Д.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВОЗМОЖНОСТИ ПОМЕХОУСТОЙЧИВЫХ КОДОВ ПО ПОВЫШЕНИЮ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ 87

Зорин К.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНТЕГРАЦИЯ ДАННЫХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ ДЛЯ ПОЛУЧЕНИЯ НОВОЙ ИНФОРМАЦИИ ... 88

Иванов В.Г., Башлаев Р.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ТРЁХМЕРНЫХ ОБЪЕКТОВ ДЛЯ УВЕЛИЧЕНИЯ ИНФОРМАТИВНОСТИ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО (СПЕЦИАЛЬНОГО) НАЗНАЧЕНИЯ 88

Иванов В.Г., Полячков А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБРАБОТКА СЛАБОСТРУКТУРИРОВАННЫХ ДОКУМЕНТОВ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В СОСТАВЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 89

Иванов М.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОПЫТ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ SDR ПРИ ДЕКОДИРОВАНИИ СИГНАЛОВ СТАНДАРТА IEEE802.11G 90

Иванов В.Г., Корякин Д.Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ В СИСТЕМАХ УПРАВЛЕНИЯ СЕТЯМИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 91

Ильина О.Б., Купчиненко О.П., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 91

Киреев С.Х.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК 92

Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Санкт-Петербургский государственный экономический университет,
Санкт-Петербургский государственный университет аэрокосмического приборостроения
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМ СОХРАНЕНИЯ ДАННЫХ..... 93

Кораблин В.О., Логинов А.А., Мач Д.П., Таран В.В., Труфанов С.К., Шерстюк М.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
ОПЕРАТИВНЫЙ КОНТРОЛЬ И РЕТРОСПЕКТИВНЫЙ АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОТЕЛЕКОММУНИКАЦИЙ..... 93

Кораблин В. О.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
СПОСОБЫ КОНТРОЛЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ ИНФОТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ..... 94

Корень М.Ю., Паршин С.И., Захаров Р.В., Гайнуллин Р.Р.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛИ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ..... 95

Коряковцев А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
КРАТКИЙ АНАЛИЗ ОШИБОК СЛЕДЯЩИХ ИЗМЕРЕНИЙ РАЗВЕДЫВАТЕЛЬНЫХ КОМПЛЕКСОВ..... 95

Купчиненко О.П., Скоропад А.В., Ильина О.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПУТИ РЕШЕНИЯ ПРОБЛЕМНЫХ ВОПРОСОВ ФОРМИРОВАНИЯ, ВЕДЕНИЯ И РАСПРОСТРАНЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЩЕГО ПОЛЬЗОВАНИЯ 96

Купчиненко О.П., Скоропад А.В., Ильина О.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ АЛГОРИТМОВ ОЦЕНКИ КАЧЕСТВА ОБСЛУЖИВАНИЯ В СЕТЯХ БЕСПРОВОДНОГО ДОСТУПА..... 97

Курашев З.В., Горячая А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДИКА ОПТИМИЗАЦИИ СЕТЕВОЙ СТРУКТУРЫВ СЕТИ ПЕРЕДАЧИ ДАННЫХ..... 97

Курашев З.В., Горячая А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АЛГОРИТМ ОПТИМИЗАЦИИ СЕТЕВОЙ СТРУКТУРЫ В СИСТЕМЕ ОБМЕНА ДАННЫМИ..... 98

Курбатов Е.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ТУРБОКОДИРОВАНИЕ И ВОЗМОЖНОСТЬ ЕГО ПРИМЕНЕНИЯ В СЕТЯХ ВОЕННОЙ СВЯЗИ..... 98

Липатников В. А., Яцкин А. Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СПОСОБ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ДИНАМИЧЕСКИХ HONEYPOT-СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ 99

Малышев В.С., Пантюхин О.И., Пащенко В.В., Терехин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 100

Манаськин А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОНТОЛОГИЧЕСКИЙ ПОДХОД К СОЗДАНИЮ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ 101

Марченко А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ НЕЙРО-НЕЧЕТКИХ СИСТЕМ С ТОЧКИ ЗРЕНИЯ ИХ ПРИМЕНЕНИЯ ДЛЯ УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ 101

Михайличенко Н.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ 102

Михеев А.А., Нешин И.Д., Опарин А.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОЕКТИРОВАНИЕ УНИВЕРСАЛЬНОГО ФОРМИРОВАТЕЛЯ ДЛЯ ПЕРСПЕКТИВНЫХ СИСТЕМ СВЯЗИ С КОСМИЧЕСКИМИ АППАРАТАМИ 103

Мордовин В.Н., Козевалин А.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОБЛЕМЫ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 104

Мошак Н.Н.
Россия, Санкт-Петербург, ПАО «Интелтех»
ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ И ЕЕ ЭЛЕМЕНТОВ 105

Муренин И.Н., Новикова Е.С.
Россия, Санкт-Петербург Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОБНАРУЖЕНИЕ АНОМАЛЬНЫХ СИТУАЦИЙ В СИСТЕМЕ АНАЛИЗА ДАННЫХ 106

Неижмак А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ОСНОВНЫХ ХАРАКТЕРИСТИК СИСТЕМ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ В КАНАЛАХ РЕГИОНАЛЬНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ И ПУТИ ИХ СОВЕРШЕНСТВОВАНИЯ 107

Нешин И.Д., Михеев А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ 108

Нешин И.Д., Опарин А.С., Михеев А.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ТЕХНОЛОГИЯ ВИРТУАЛЬНОГО ТУРА КАК ИНСТРУМЕНТ ДЛЯ ОБУЧЕНИЯ 108

Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МОДЕЛИ ВИЗУАЛЬНОГО АНАЛИЗА СЕТЕВЫХ ПОТОКОВ КОМПЬЮТЕРНОЙ СЕТИ 109

Ноздрачёв Л.И. Бударин Э.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 110

Овсянников С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОДХОДЫ К МОДЕЛИРОВАНИЮ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЛАНИРОВАНИИ СЕТИ БЕСПРОВОДНОГО АБОНЕНТСКОГО ДОСТУПА..... 110

Олимпиев А.А.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
МЕТОДИКА ФОРМИРОВАНИЯ КОМПОНЕНТОВ МЕТАИНФОРМАЦИИ ДЛЯ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ ЭЛЕМЕНТА СЕТИ СВЯЗИ С УПРАВЛЯЕМОЙ ТОЧНОСТЬЮ..... 111

Олимпиев А. А., Шерстюк Ю. М.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
МЕТОДИКА ПОСТРОЕНИЯ И АДАПТАЦИИ СИНТАКСИЧЕСКИ ВАРИАНТНОЙ СИСТЕМЫ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО МОНИТОРИНГА 112

Панков Р.Н., Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОСНОВЫ ФОРМИРОВАНИЯ ПОЛЕВОЙ КОМПОНЕНТЫ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ..... 113

Паращук И.Б., Дедюрин А.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ GPGPU ДЛЯ ПРОИЗВЕДЕНИЯ НЕГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ..... 114

Паращук И.Б., Царамов М.В., Сафонов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ОСНОВНЫХ ТРЕБОВАНИЙ К ПРОЦЕДУРАМ ПОИСКА И НАВИГАЦИИ В БОЛЬШИХ ОБЪЕМАХ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 115

Паращук И.Б., Домбровский Я.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СУЩНОСТЬ ОБЕСПЕЧЕННОСТИ И УДОБСТВА ИСПОЛЬЗОВАНИЯ КАК КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ПРОЦЕССА ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 115

Паращук И.Б., Гнедь Е.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОДХОД К ФОРМУЛИРОВКЕ ПОКАЗАТЕЛЕЙ ДЕЙСТВЕННОСТИ ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ РЕГИОНАЛЬНЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 116

Паращук И.Б., Михайличенко Н.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
НЕЙРО-НЕЧЕТКИЕ МОДЕЛИ В ИНТЕРЕСАХ УПРАВЛЕНИЯ ДАННЫМИ В ЦОД И ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ИНФОРМАЦИИ В РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ..... 117

Подниколенко А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ MPLS-TP В ТРАНСПОРТНЫХ СЕТЯХ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ 118

Полугина Ю.К.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МЕТОДЫ ОЦЕНКИ КАЧЕСТВА VOIP СВЯЗИ 118

Присяжнюк С.П., Зализнюк А.Н.
Россия, Санкт-Петербург, АО Институт телекоммуникаций
г. Москва, Военно-топографического управления Генерального штаба Вооруженных Сил РФ
НАПРАВЛЕНИЯ РАЗВИТИЯ СТРАТЕГИЧЕСКОГОГО ПЛАНИРОВАНИЯ ГЕОИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СИСТЕМ УПРАВЛЕНИЯ 119

Разинов А.А., Иванов В.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРЕДЛОЖЕНИЯ ПО СОСТАВУ ПРОГРАММНО- ТЕХНИЧЕСКОГО КОМПЛЕКСА ОРГАНОВ УПРАВЛЕНИЯ СВЯЗЬЮ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИИ 120

Репников А.Ю., Пустошкин М.М., Худайназаров Ю.К.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПЕРЕСЕКТИВЫ РАЗВИТИЯ СРЕДСТВ РАДИОМОНИТОРИНГА 121

Сабуров А.В., Крючков Д.В., Бегмахмудов И.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ПЕРЕДАЧИ РЕЧЕВЫХ СООБЩЕНИЙ С КОММУТАЦИЕЙ ПАКЕТОВ ПО IP-СЕТЯМ 122

Савенков С.Н., Ногин С.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВИРТУАЛИЗАЦИЯ ОБРАБОТКИ ДАННЫХ 123

Сазонов В.В., Арсентьев А.И., Мосягин Д.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СЕТИ РАДИОСВЯЗИ . 124

Сазонов В.В., Титов В.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРЕДЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СИСТЕМ ДОКУМЕНТАЛЬНОГО ОБМЕНА 124

Сапунова Л.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛЬ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ С МЯГКИМ ДЕКОДИРОВАНИЕМ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ 125

Сафронов Ю.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ СО СПЕКТРАЛЬНЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ПРОИЗВОДСТВА 126

Саяркин Л.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ. АВТОМАТИЗИРОВАННЫЕ РАБОЧИЕ МЕСТА УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ, АНАЛИЗ ИХ УЯЗВИМОСТЕЙ И ОЦЕНКА НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 126

Сидорова А.П., Боровкова М.А., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ОТКРЫТОГО СЕГМЕНТА ОАЦСС НА ОСНОВЕ SIEM-ТЕХНОЛОГИИ 127

Сныткин И.И., Кулюпин Е.Н.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ПЕРСПЕКТИВНЫХ СИСТЕМ ДВУКРАТНЫХ ПРОИЗВОДНЫХ КОДОВЫХ ДИСКРЕТНО-ЧАСТОТНЫХ СИГНАЛОВ С ЗАДАННЫМИ СВОЙСТВАМИ И АППАРАТНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЕЕ РЕАЛИЗАЦИИ 128

Сныткин И.И., Балюк А.А.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М.Штеменко
МЕТОД АНАЛИЗА И РАСКРЫТИЯ "ТОНКОЙ" ВНУТРЕННЕЙ СТРУКТУРЫ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ 128

Сныткин И.И., Енин Н.Н.
Россия, г. Краснодар, Краснодарское высшее военное училище имени генерала армии С.М.Штеменко
НОВЫЕ ПРИНЦИПЫ И МЕТОД ЭФФЕКТИВНОЙ АДРЕСАЦИИ СТРУКТУРНЫХ ЭЛЕМЕНТОВ ПАКЕТНЫХ СЕТЕЙ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ПРИМЕНЕНИЯ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ НЕЛИНЕЙНОЙ СТРУКТУРЫ 129

Соловьев В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ ПРОБЛЕМЫ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ 129

Старков А.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОБЛЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ 130

Троянов Я.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ХЭШ-ФУНКЦИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МЕХАНИЗМОМ 131

Труфанов С.К., Шерстюк М.Ю., Мач Д.П.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
ТИПОВЫЕ МЕТОДЫ ОБРАБОТКИ ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА ИНФОТЕЛЕКОММУНИКАЦИЙ 132

Тюмин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОЦЕНКА СВОЕВРЕМЕННОСТИ ПЕРЕДАЧИ СИГНАЛОВ БОЕВОГО УПРАВЛЕНИЯ И ОПОВЕЩЕНИЯ 133

Фёдоров П.Н., Сазонов В.В., Зубакин В.В., Ванчугов А.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
О НЕОБХОДИМОСТИ РАЗРАБОТКИ ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ ОБМЕНА ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 133

Федотов Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОДХОД К ВЫЯВЛЕНИЮ АНОМАЛИЙ В МАССИВЕ ДАННЫХ ОТ РАЗНЫХ ИСТОЧНИКОВ ДАННЫХ 134

Фисенко М.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОЦЕНКА ЖИВУЧЕСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ 135

Харитоненко В.Г.
Россия, г. Краснодар, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко
ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЯ ПРИ ИДЕНТИФИКАЦИИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ 135

Хушкин Д.П., Ноздрачёв Л.И., Бударин Э.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ВОЙНЫ 136

Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек-Балтика М»
ОСНОВНЫЕ ПРОФИЛИ БАЗОВОЙ ТЕХНИЧЕСКОЙ АРХИТЕКТУРЫ АСУ СВЯЗЬЮ 137

Шерстюк К.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
СПОСОБЫ ЦЕНТРАЛИЗОВАННОГО ОБНОВЛЕНИЯ УСЛОВНО-ПОСТОЯННЫХ ДАННЫХ В ИЕРАРХИЧЕСКИ ОРГАНИЗОВАННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 138

Шерстюк Ю.М.
Россия, Санкт-Петербург, АО «Инфотек-Балтика М»
СОБЫТИЙНО-ОРИЕНТИРОВАННОЕ ПОСТРОЕНИЕ ПРОЦЕССОВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ИНФОТЕЛЕКОММУНИКАЦИЯМИ 139

Шерстюк М.Ю.
Россия, Санкт-Петербург, АО «Институт инфотелекоммуникаций»
МЕТОД ХРАНЕНИЯ ФАКТОГРАФИЧЕСКИХ ДАННЫХ В РЕЛЯЦИОННЫХ ТАБЛИЦАХ 140

Шипицын Д. Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АКТУАЛЬНОСТЬ И ПРОБЛЕМАТИКА ВНЕДРЕНИЯ МЕХАНИЗМОВ ПРИОРИТИЗАЦИИ ПАКЕТНОГО ТРАФИКА В СТАЦИОНАРНЫХ СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ 140

Широков В.В., Егоров С.С., Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МЕТОДОЛОГИЯ ПРИКЛАДНОГО ИСПОЛЬЗОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ 141

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 143

Алексеев И.В., Зегжда П.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ВЫЯВЛЕНИЕ ЗАШИФРОВАННЫХ ИСПОЛНЯЕМЫХ ФАЙЛОВ НА ОСНОВЕ АНАЛИЗА ЭНТРОПИИ СЕКЦИЙ ИСПОЛНЯЕМЫХ ФАЙЛОВ ФОРМАТА PE32 143

Баранов С.Н., Тележкин А.М., Мустафин Н.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
УПРАВЛЕНИЕ РИСКАМИ В ПРОГРАММНЫХ ПРОЕКТАХ 144

Башмаков А.В., Когтев А.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
УГРОЗЫ ПРОСЛУШИВАНИЯ И НЕГЛАСНОГО СЪЁМА ИНФОРМАЦИИ С МОБИЛЬНЫХ ТЕЛЕФОНОВ 144

Белоусов Н.С.
Россия, г. Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПЕРСОНАЛЬНЫЕ ДАННЫЕ СОТРУДНИКОВ, ОБРАБАТЫВАЕМЫХ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСИТЕМАХ 145

Бойченко О.В., Тупота Е.С.
Россия, г. Крым, Крымский федеральный университет имени В.И. Вернадского
ТЕХНОЛОГИИ DATA LEAK PREVENTION В СИСТЕМЕ ЗАЩИТЫ КОММЕРЧЕСКИХ ДАННЫХ 146

Бойченко О.В, Дячук В.С.
Россия, г. Крым, Крымский федеральный университет имени В.И. Вернадского
СПОСОБЫ ЗАЩИТЫ ДАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭЛЕКТРОЭНЕРГЕТИКЕ 147

Башмаков А.В., Проноза А.А., Романов Е.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРИМЕНЕНИЕ ЭКОСИСТЕМЫ БОЛЬШИХ ДАННЫХ ПРИ ИССЛЕДОВАНИИ СОЦИАЛЬНЫХ СЕТЕЙ В ЦЕЛЯХ ВЫЯВЛЕНИЯ УГРОЗ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ 148

Большакова Л.В., Дементьева А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
О ВЛИЯНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ФАКТОРОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РОССИИ 149

Большакова Л.В., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
МНОГОКРИТЕРИАЛЬНАЯ ОПТИМИЗАЦИЯ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 149

Браницкий А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
КОМБИНИРОВАННЫЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК НА ОСНОВЕ СИГНАТУРНОГО АНАЛИЗА И МЕТОДОВ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА 150

Браницкий А.А., Коломеец М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
РАЗРАБОТКА СИСТЕМЫ ВИЗУАЛИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ДИАГРАММЫ ВОРОНОГО 150

Булгаков М.В., Чечулин А.А
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ МОДЕЛИРОВАНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В СИСТЕМАХ ЖЕЛЕЗНОДОРОЖНОГО ДВИЖЕНИЯ 151

Бурлов В.Г., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
СИНТЕЗ МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМ УЧРЕЖДЕНИЕМ С ИСПОЛЬЗОВАНИЕМ АНАЛИТИЧЕСКО-ДИНАМИЧЕСКОЙ МОДЕЛИ И ИНТЕРНЕТ ТЕХНОЛОГИЙ .. 152

Бухарметов М.Р., Ныркov А.П.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
О БЕЗОПАСНОСТИ КАНАЛОВ СВЯЗИ СИСТЕМ МОНИТОРИНГА ВОДНОГО ТРАНСПОРТА 152

Винокурова А. И., Ермачкова В. И., Спивак А.И.
Россия, Санкт-Петербург, Университет ИТМО
ПРИМЕНЕНИЕ МОДЕЛЕЙ АТАК НА ОБЕЗЛИЧЕННЫЕ ДАННЫЕ В СИСТЕМЕ ЗАЩИТЫ БАЗ ДАННЫХ 153

Домбровская Л.А., Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИСПОЛЬЗОВАНИЕ МИКРОПРОЦЕССОРОВ И КРИПТОГРАФИЧЕСКИХ МИКРОСХЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ 153

Демидов Р.А., Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПАРАЛЛЕЛИЗАЦИЯ ПОИСКА УЯЗВИМОСТЕЙ В БИНАРНОМ КОДЕ С ИСПОЛЬЗОВАНИЕМ КЛАСТЕРНЫХ ВЫЧИСЛЕНИЙ 154

Десницкий В.А., Александров В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ 155

Десницкий В.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МЕТОДИКИ ВЕРИФИКАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ 156

Дремов А.С., Павленко Е.Ю., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПРИМЕНЕНИЕ МЕТОДОВ ДИНАМИЧЕСКОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СПАМА В СОЦИАЛЬНЫХ СЕТЯХ 157

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ОЦЕНКА ЗАЩИЩЕННОСТИ НА ОСНОВЕ ГРАФОВ И ОТКРЫТЫХ СТАНДАРТОВ ДЛЯ СЕТЕЙ С МОБИЛЬНЫМИ КОМПОНЕНТАМИ 158

Ежгуров В.Н., Петров С.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
БАЗОВЫЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ МОБИЛЬНЫХ УСТРОЙСТВ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ НА БАЗЕ СИММЕТРИЧНЫХ И АСИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ 159

Ерисова А.Д.
Россия, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова
ИСТОРИЯ И МЕТОДЫ АУТЕНТИФИКАЦИИ 159

Жуковский Е.В., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В БИНАРНОМ КОДЕ 160

Зегжда Д.П., Зегжда П.Д., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПРОБЛЕМЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ В СЕТЯХ ТРАНСПОРТНЫХ СРЕДСТВ 161

Зуров Е.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОЦЕНКА ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ЗЛОУМЫШЛЕННИКОМ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ 162

Иванов Д.В., Москвин Д.А., Овасапян Т.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ИССЛЕДОВАНИЕ МЕТОДОВ АУДИТА БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТ НА ОСНОВЕ ОБНАРУЖЕНИЯ АКТИВНЫХ УЗЛОВ IPV6-АДРЕНОГО ПРОСТРАНСТВА 163

Ильченко Л.М. Зайцев С.И.
Российская Федерация, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова
ПОНЯТИЙНЫЙ АППАРАТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ 163

Ильченко Л.М. Зайцев С.И.
Россия, Санкт-Петербург, ГУМРФ им. адмирала С.О. Макарова
ОЦЕНКА ОПАСНОСТИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 165

Келесис Н.В.
Россия, Санкт-Петербург, Университет ИТМО
РАЗРАБОТКА МЕТОДА ПОИСКА WEB-УЯЗВИМОСТЕЙ ПРИ ПРОВЕДЕНИИ АУДИТА ЗАЩИЩЕННОСТИ 166

Коломеец М.В., Чечулин А.А., Копчак Я.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»
РАЗРАБОТКА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА СИСТЕМЫ ВИЗУАЛИЗАЦИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ ... 166

Комашинский Н.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АНАЛИЗ ПОДХОДОВ ДЛЯ ОБНАРУЖЕНИЯ ЦЕЛЕВЫХ АТАК ... 167

Коротков В.В.
Россия. Санкт-Петербург. ГУМРФ им. адм. С.О. Макарова
ЕДИНЫЙ ПОДХОД К ИЗМЕРЕНИЯМ ПО КОНТРОЛЮ ЗАЩИЩЕННОСТИ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ ... 168

Котенко И.В., Ушаков И.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Санкт-Петербургский институт информатики и автоматизации РАН
ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ ДЛЯ МОНИТОРИГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ... 168

Левшун Д.С., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ЗАЩИЩЕННОЕ МЕЖКОНТРОЛЛЕРНОЕ ВЗАИМОДЕЙСТВИЕ НА БАЗЕ ПРОТОКОЛА I2C ... 169

Левоневский Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
РАСПОЗНАВАНИЕ ОБРАЗОВ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ... 170

Лемец А.А., Павленко Е.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
АНАЛИЗ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ SSL PINNING В ПРИЛОЖЕНИЯХ ДЛЯ ОС GOOGLE ANDROID ... 171

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, ООО «Газинформсервис»,
Республика Беларусь, г. Минск, УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД
СОСТОЯНИЕ ВОПРОСА ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИМПОРТОЗАМЕЩЕНИИ ... 172

Лопатин Д.В., Анурьева М.С., Остапчук К.И., Ерёмина Е.А., Пузанова Я.М., Житенева И. А.
Россия, г. Тамбов, Тамбовский государственный университет имени Г.Р. Державина
ПРОБЛЕМА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ УГРОЗ В РЕГИОНЕ ... 174

Макаров А.С., Москвин Д.А. Иванов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
РАЗРАБОТКА ЗАЩИЩЁННОГО USB НАКОПИТЕЛЯ ... 175

Малов С.С., Юмашева Е.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ... 176

Малышев Е.В., Павленко Е.Ю., Зегжда П.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ВЫЯВЛЕНИЕ АВТОМАТИЧЕСКИ УПРАВЛЯЕМЫХ УЧЕТНЫХ ЗАПИСЕЙ В СОЦИАЛЬНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ ... 177

Марков В.С., Сидоренко Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский научный центр Российской академии наук
СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ... 178

Меркушев Е.С., Котенко И.В.
Россия, Санкт-Петербург, Санкт Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
АНАЛИЗ СВОЙСТВ ЭКОСИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ 179

Минин А.А., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
УГРОЗЫ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ДИНАМИЧЕСКИХ СЕТЕЙ VANET/MANET 180

Минин А.А., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
МЕТОД ЗАЩИТЫ ОТ УГРОЗ ДОСТУПНОСТИ СЕТЕЙ ТИПА M2M ПУТЕМ ДИНАМИЧЕСКОЙ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ 180

Михайлов М.В., Чечулин А.А.
Россия, г. Ярославль, Ярославский государственный университет им. П.Г. Демидова, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
КЛАСТЕРИЗАЦИОННО-КОРРЕЛЯЦИОННЫЙ СКАНЕР ХРАНИЛИЩА ДАННЫХ 181

Москвин Д.А., Мясников А.В.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
СИНХРОНИЗАЦИЯ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ ПО БЕЗОПАСНОМУ КАНАЛУ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ NFC 182

Москвин Д.А., Дахнович А.Д.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
СХЕМА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ МЕЖДУ КЛИЕНТАМИ И ТОЧКАМИ ДОСТУПА Wi-Fi 182

Никитин А.С., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПРОТИВОДЕЙСТВИЕ АТАКАМ ДЕАНОНИМИЗАЦИИ В АНОНИМНОЙ СЕТИ TOR НА ОСНОВЕ СТАТИСТИЧЕСКИХ ИССЛЕДОВАНИЙ 183

Новожилов Д.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МЕТРИКИ ДЛЯ АНАЛИЗА СТРУКТУРНЫХ ОСОБЕННОСТЕЙ ВЕБ-СТРАНИЦ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ 184

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА 185

Парфенов Н.П., Сударев В.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
НЕКОТОРЫЕ МЕРЫ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ 186

Попова А.Н.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
К ВОПРОСУ О ПОИСКАХ УЯЗВИМОСТЕЙ В ИНТЕРНЕТ-СИСТЕМАХ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ 187

Проноза А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АНАЛИЗ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ БОЛЬШИХ ДАННЫХ ДЛЯ РЕШЕНИЯ ЗАДАЧИ МОНИТОРИНГА КРУПНОМАСШТАБНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 188

Проноза А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВИЗУАЛИЗАЦИИ БОЛЬШИХ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ 189

Резединова Е.Ю., Кожушко Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
МЕТОДЫ СЕНТИМЕНТ-АНАЛИЗА ВЫСКАЗЫВАНИЙ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ TWITTER 190

Романова Ю.Н., Янюшкин К.А., Нырков А.П.
Россия, Санкт-Петербург, Университет ИТМО, ГУМРФ им. адм. С.О. Макарова
О ПРИМЕНЕНИИ ОТЕЧЕСТВЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ 191

Резединова Е.Ю., Ушанова И.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПОДБОР ФОРМАЛЬНЫХ ПРИЗНАКОВ ДЛЯ АВТОМАТИЗАЦИИ ПОИСКА БОТОВ
В СОЦИАЛЬНЫХ СЕТЯХ 191

Саенко И.Б., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИ И МЕТОДЫ ВИЗУАЛЬНОГО АНАЛИЗА СХЕМ И ПОЛИТИК РАЗГРАНИЧЕНИЯ ДОСТУПА
К РЕСУРСАМ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА 192

Саенко И.Б., Кушнеревич А.Г., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и
автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»
ПЛАТФОРМА ПАРАЛЛЕЛЬНОГО РАСПРЕДЕЛЕННОГО АНАЛИЗА ТРАФИКА В
КОМПЬЮТЕРНЫХ СЕТЯХ ДЛЯ ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ 193

Саликов А.В.
Россия, Санкт – Петербург, Санкт-Петербургский Университет МВД России
БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ 194

Стахно Р.Е., Ковалёв В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ О ЗАЩИТЕ ПОТОКОВ ДАННЫХ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ 195

Супрун А.Ф., Туманов Н.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА ИНФОРМАЦИИ ВЫСОКОЙ СТЕПЕНИ ЗАЩЕННОСТИ 196

Теплов Э.П., Кардакова М.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
АКТУАЛЬНЫЕ ВОПРОСЫ СОЦИОКУЛЬТУРНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
С СИСТЕМНЫХ ПОЗИЦИЙ 196

Усов Е.С., Никольский А.В., Павленко Е.Ю., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ОБЛАЧНЫХ СИСТЕМ
С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ INTEL SGX 197

Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики
и автоматизации РАН
ПОСТРОЕНИЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ 198

Федорченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации
Российской академии наук
ХОСТ-ОРИЕНТИРОВАННАЯ МЕТОДИКА КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ 199

Хитов С.Б., Еременко С.П., Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербургский университет МВД России
К ВОПРОСУ ОБ ОЦЕНКЕ ЗАЩИЩЕННОСТИ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ 200

Хитов С.Б., Еременко С.П., Смирнова О.Г.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербургский университет МВД России
НЕКОТОРЫЕ АСПЕКТЫ ОБОСНОВАНИЯ СРЕДСТВ ФИНАНСОВГО ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ 201

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТРИЧЕСКАЯ ОЦЕНКА ФАКТОРОВ РИСКА НА ОСНОВЕ СТРУКТУРНОЙ ИНФОРМАЦИИ ПРИ КОГНИТИВНОМ ПОДХОДЕ 201

Юмашева Е.С., Теплов Э.П.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ИНФОРМАЦИОННЫЕ УГРОЗЫ ОРГАНИЗАЦИИ С ПОЗИЦИИ СИСТЕМНОГО АНАЛИЗА И РУССКОЙ ЛИТЕРАТУРЫ 202

Ярмак А.В., Павленко Е.Ю., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ОЦЕНКА БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ НА ОСНОВЕ НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ 203

ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИ 205

Березкина Е.Н.
Россия, Санкт-Петербург, Информационный центр Главного управления МВД РФ по г. Санкт-Петербургу и Ленинградской области
ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ ПРИНЯТИИ РЕШЕНИЯ О ВСТУПЛЕНИИ ГРАЖДАН В ОБЩЕСТВЕННЫЕ ОБЪЕДИНЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ НАПРАВЛЕННОСТИ 205

Бойкова Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ ОСНОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ МВД РОССИИ В ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ЛИЦЕНЗИОННО-РАЗРЕШИТЕЛЬНОЙ РАБОТЫ 206

Бурлов В.Г., Дмитриева А.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА МОДЕЛИ АРМ РУКОВОДИТЕЛЯ ГРУППЫ ЭКСПЕРТОВ ОВД НА ОСНОВЕ МЕТОДА ДЕЛЬФИ 207

Бурлов В.Г., Павлина Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ НА ТИПОВОМ ПЕРЕКРЕСТКЕ МЕГАПОЛИСА 208

Бурлов В.Г., Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА МОДЕЛИ АРХИТЕКТУРЫ ЭВМ, ФУНКЦИОНИРУЮЩЕЙ В УСЛОВИЯХ РАЗРУШЕНИЯ ПРОГРАММНОЙ СРЕДЫ 208

Вождаев А.В., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРОБЛЕМЫ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОВД 209

Егорова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА ЭЛЕМЕНТОВ СИСТЕМЫ, АВТОМАТИЗИРУЮЩЕЙ ПРОЦЕСС ОХРАНЫ КВАРТИР И КОТТЕДЖЕЙ 210

Ефимова А.Б.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
ПОДГОТОВКА ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА ВОЕННЫХ ИНСТИТУТОВ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ К ПРИМЕНЕНИЮ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ 211

Зайцева Е.А., Ланг Т.Е.
Россия, Санкт-Петербург, Санкт-Петербургский институт внутренних войск МВД России,
Санкт-Петербургский университет МВД России
МЕТОДЫ СБОРА ИНФОРМАЦИИ О ГРАЖДАНАХ РОССИЙСКОЙ ФЕДЕРАЦИИ 212

Зайцева Е.А., Попова А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ 213

Зингачева Д.А., Чудаков О.Е., Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА ИНТЕРАКТИВНОГО ПРАКТИЧЕСКОГО ЗАНЯТИЯ ПО ДИСЦИПЛИНЕ «ПРОГРАММИРОВАНИЕ» 214

Иванов А.Ю., Редковников В.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА АРМ ПРЕПОДАВАТЕЛЯ КАФЕДРЫ СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ 215

Иванов А.Г., Куватов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
РАЗРАБОТКА ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ОФИЦЕРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ МВД РФ 216

Кадулин В.Е.
Россия, г. Москва, Московский университет МВД России
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 216

Колесов Д.А., Куватов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
РАЗРАБОТКА ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА РУКОВОДИТЕЛЯ ПОДРАЗДЕЛЕНИЯ ОВД 217

Куватов В.И., Потехин В.С., Чудаков О.Е.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ИТ), ОБЕСПЕЧИВАЮЩИХ АВТОМАТИЗАЦИЮ ПРОЦЕССОВ ПОИСКА УГНАННЫХ АВТОТРАНСПОРТНЫХ СРЕДСТВ 218

Куватов В.И., Синещук Ю.И., Синещук М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России
ПРОБЛЕМА ВЫБОРА РАЦИОНАЛЬНОГО СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ 219

Куватов В.И., Скрипниченко А.Ю., Санкт-Петербургский университет МВД России
РАЗРАБОТКА СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ОТДЕЛА ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ С ВНЕДРЕНИЕМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОХРАНЫ И СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ 220

Малов С.С., Юмашева Е.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
О КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ 221

Потехин В.С., Ващилова А.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ПУТИ СОЗДАНИЯ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ (ИТ), ОБЕСПЕЧИВАЮЩЕЙ РЕАЛИЗАЦИЮ ПЛАНА «ПЕРЕХВАТ» 222

Потехин В.С., Никифорова А.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ПОДХОД К АВТОМАТИЗАЦИИ КОНТРОЛЯ ДОСТУПА НА ОСОБО ВАЖНЫЕ ОБЪЕКТЫ 223

Потехин В.С., Харрасов Э.Э.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОИСКА УГНАННОГО АВТОТРАНСПОРТА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ РАДИОМЕТОК 224

Примакин А.И., Чудаков О.Е., Рыжков Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ТЕХНОЛОГИЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО НАЧАЛЬНИКА КАФЕДРЫ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ..... 224

Родин В.Н., Томашевич Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ОБОСНОВАНИЕ И ВЫБОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОБЪЕКТОВ ОВД 226

Савченко-Новопавловская С.Л., Дикий Д.И.
Россия, Санкт-Петербург, Университет ИТМО
ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ 227

Синещук Ю.И., Конопак А.Е.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России
ОРГАНИЗАЦИЯ ЗАЩИЩЕННЫХ КАНАЛОВ СВЯЗИ НА БАЗЕ ТЕХНОЛОГИИ VIPNET В МЧС РОССИИ 227

Синещук Ю.И., Левчунец И.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России
ОБОСНОВАНИЕ СИСТЕМЫ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В МНОГОУРОВНЕВОЙ НАВИГАЦИОННО-ИНФОРМАЦИОННОЙ СИСТЕМЕ МОНИТОРИНГА ТРАНСПОРТНЫХ СРЕДСТВ МЧС РОССИИ НА БАЗЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ГЛОНАСС..... 228

Соловейчик М.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ-ПОИСКОВЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ДЕЯТЕЛЬНОСТИ ЦЕНТРОВ ВРЕМЕННОГО СОДЕРЖАНИЯ НЕСОВЕРШЕННОЛЕТНИХ ПРАВОНАРУШИТЕЛЕЙ..... 229

Хомченкова А.О., Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗАЦИИ КОНТРОЛЯ ПРОЦЕССА УПРАВЛЕНИЯ ПРИБЫТИЯ ЛИЧНОГО СОСТАВА ПО ТРЕВОГЕ В УНИВЕРСИТЕТ МВД РФ 230

Чудаков О.Е., Хахель С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
РАЗРАБОТКА ЭЛЕМЕНТОВ СИСТЕМЫ, АВТОМАТИЗИРУЮЩИХ ПРОЦЕСС ВЫЯВЛЕНИЯ И УЧЕТА ПРАВОНАРУШЕНИЙ НА ВОДНЫХ МАГИСТРАЛЯХ ГОРОДА С ИСПОЛЬЗОВАНИЕМ КВАДРОКОПТЕРОВ..... 231

Целовальников Н.А., Пушкина О.А., Пенкин Д.Д.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
КОМПЛЕКСНАЯ ОЦЕНКА ДЕЯТЕЛЬНОСТИ КУРСАНТОВ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА (НА ПРИМЕРЕ КЛАСТЕРНОГО АНАЛИЗА)..... 232

Якушев Д.И., Жидкова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
АВТОМАТИЗАЦИЯ ПРОЦЕССА СБОРА ДАННЫХ РЕЗУЛЬТАТОВ ПРОТОКОЛИРОВАНИЯ СОБЫТИЙ БЛИЗ ДВИЖУЩЕГОСЯ ОБЩЕСТВЕННОГО ТРАНСПОРТА..... 233

Якушев Д.И., Иванова Е.А., Мордовина А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
ПРИМЕНЕНИЕ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА (НА ПРИМЕРЕ КЛАСТЕРНОГО АНАЛИЗА) В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОВД 233

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ 235

Алексеев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОБЩИЙ ИНФОРМАЦИОННЫЙ РЕСУРС, ФУНКЦИИ И ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ПОДРАЗДЕЛЕНИЯМИ ОВД 235

Баранов Н.А.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ИНФОРМАЦИОННАЯ ПОЛИТИКА РОССИИ В КОНТЕКСТЕ КОНЦЕПЦИИ «МЯГКОЙ СИЛЫ» 236

Блохина М.Ю.
Россия, Санкт-Петербург, Университет ИТМО
ИСПОЛЬЗОВАНИЕ ОБРАТНОГО ПРОЕКТИРОВАНИЯ В РАМКАХ МОДЕРНИЗЩАЦИИ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ 237

Лепёхин А.Н.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь
О ФОРМИРОВАНИИ МЕТОДОЛОГИЧЕСКИХ ОСНОВ ПРИ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 237

Бурлов В.Г., МокееваТ.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макаров
РАЗРАБОТКА ДИНАМИЧЕСКОЙ МОДЕЛИ УПРАВЛЕНИЯ В СОЦИАЛЬНОЙ И ЭКОНОМИЧЕСКОЙ СИСТЕМЕ 238

Чикунов В.В.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь
О ПОНЯТИИ И СОДЕРЖАНИИ ИНФОРМАЦИИ В КОНТЕКСТЕ ПРОВЕДЕНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 239

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 241

Глебов Н.Б., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК УГРОЗА БЕЗОПАСНОСТИ ОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ В ОРГАНИЗАЦИИ 241

Глебов Н.Б., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ 241

Забарин А.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД РФ
МАССОВЫЕ БЕСПОРЯДКИ КАК КОГНИТИВНЫЕ ТЕХНОЛОГИИ СЕТЕВЫХ ВОЙН 242

Кефели И.Ф.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ИДЕОЛОГЕМА «РУССКИЙ МИР» В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОМ ПРОТИВОБОРСТВЕ 243

Колотов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ТЕХНОЛОГИИ ВЕДЕНИЯ ГИБРИДНЫХ ВОЙН НА ДАЛЬНЕМ ВОСТОКЕ В ИСТОРИЧЕСКОЙ РЕТРОСПЕКТИВЕ 244

Комлева Н.А.
Россия, Екатеринбург, Центр геополитического анализа
ИДЕОЛОГИЧЕСКАЯ ГРАНИЦА КАК ПРЕДЕЛ БЕЗОПАСНОСТИ ИДЕОЛОГИЧЕСКОГО ПРОСТРАНСТВА 244

Мельник Г.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ТАКТИЧЕСКИЕ МЕДИА КАК УГРОЗА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ 245

Плебанек О.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф.Устинова
КОГНИТИВНО-АКСИОЛОГИЧЕСКИЕ МЕХАНИЗМЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА 246

Попов П.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова
ИДЕОЛОГЕМА КАК ЭЛЕМЕНТ ГИБРИДНОЙ ВОЙНЫ 246

Самуйлова И.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
РОЛЬ КАЧЕСТВА СООБЩЕНИЙ МАСС-МЕДИА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА 247

Свешникова Н.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПСИХОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ..... 248

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ 249

Большакова Л.В., Грачев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРОВЕРКА АДЕКВАТНОСТИ ПОСТРОЕННЫХ ЭКОНОМЕТРИЧЕСКИХ МОДЕЛЕЙ..... 249

Васькова А.В., Михайличенко Е.М.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации
МНОГОФАКТОРНАЯ МОДЕЛЬ ДЮПОН АНАЛИЗА ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ НА ПРИМЕРЕ ОАО «АВТОВАЗ» И ОАО «ГАЗ» 249

Верзун Н.А., Касаткин В.В., Колбанёв М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский институт информатики и автоматизации РАН
ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ И КИБЕРФИЗИКОБИОЛОГИЧЕСКИЕ ПРОИЗВОДСТВЕННЫЕ СИСТЕМЫ 251

Верзун Н.А., Колбанёв М.О, Омельян А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СИСТЕМА РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ДЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РУСУРСАМ..... 251

Володина А.А., Левкин И.М.
Россия, Санкт-Петербург, Университет ИТМО
МОДЕЛЬ ФОРМИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ ИНФОРМАЦИОННОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ 252

Головкин Ю.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОДЕЛИРОВАНИЕ ПРОЦЕССОВ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ СЛОЖНЫМИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ В НЕШТАТНЫХ СИТУАЦИЯХ..... 252

Елизаров М.А. Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОДЕЛЬ ИДЕНТИФИКАЦИИ МЕТОК В RFID-СИСТЕМЕ 253

Емельянов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ПРИМЕНЕНИЕ СЕТЕВЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ ПРЕДПРИЯТИЙ МАЛОГО БИЗНЕСА..... 254

Касаткин В.В., Колбанёв М.О., Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный экономический университет
АНАЛИЗ ПРОЦЕССОВ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ ДАННЫХ..... 255

Килин В.С.
Россия, Санкт-Петербург, Университет ИТМО
РЫНОК ИТ-АУТСОРСИНГА В СТРУКТУРЕ ЭКОНОМИЧЕСКОЙ СИСТЕМЫ..... 255

Коломойцев В.С.
Россия, Санкт-Петербург, Университет ИТМО
О ПРОБЛЕМЕ ПРОЕКТИРОВАНИЯ БЕЗОПАСНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ..... 256

Кузьмина Е.И.
Россия, Санкт-Петербург, Санкт- Петербургский государственный экономический университет
ФЕНОМЕН ЭФФЕКТИВНОСТИ КОМПАНИИ ALIBABA GROUP ДЖЕКА МА 257

Левкин И.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЗНАЧИМОСТИ ИНФОРМАЦИОННЫХ ПРОДУКТОВ (УСЛУГ) 257

Левкин И.М.
Россия, Санкт-Петербург, Университет ИТМО
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ ФОРМИРОВАНИЙ МЧС В РАЙОНАХ
КРУПНОМАСШТАБНЫХ КАТАСТРОФ 258

Левкина С.В.
Россия, Санкт-Петербург, ООО «Витамед»
ЧИСЛЕННАЯ ОЦЕНКА ЦЕННОСТИ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ 259

Минаков В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УМНЫХ ИННОВАЦИЯХ: ПРИЗНАКИ, СВОЙСТВА 259

Михайлова А.С.
Россия, Санкт-Петербург, Балтийский государственный технический университет
«ВОЕНМЕХ» им. Д.Ф. Устинова
СИСТЕМА МОТИВАЦИИ ПЕРСОНАЛА НА ПРЕДПРИЯТИИ 260

Михайличенко Е.М., Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет
им. А. И. Герцена, Финансовый университет при Правительстве Российской Федерации,
Санкт-Петербургский государственный институт психологии и социальной работы
ТЕХНОЛОГИИ «ИНТЕРНЕТ - МАРКЕТИНГА» КАК СРЕДСТВО ПОВЫШЕНИЯ
КОНКУРЕНТОСПОСОБНОСТИ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ 260

Николаев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ИНФОРМАЦИОННЫЕ РИСКИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА: АНАЛИЗ УГРОЗ
И УЯЗВИМОСТЕЙ 261

Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОБ ОДНОМ ПОДХОДЕ К ФОРМИРОВАНИЮ СПЕЦИАЛНЫХ ДИСЦИПЛИН ВАРИАТИВНОЙ ЧАСТИ
ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ 262

Останина М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ФРЕЙМВОРК УПРАВЛЕНИЯ БИЗНЕС-ИНФОРМАЦИЕЙ BISL 263

Соколов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА..... 263

Тюрликов А.М., Татарникова А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
аэрокосмического приборостроения
СИСТЕМА ОБНАРУЖЕНИЯ ПАТОЛОГИЙ ОПОРНО-ДВИГАТЕЛЬНОГО АППАРАТА С
ПОМОЩЬЮ АКСЕЛЕРОМЕТРОВ МОБИЛЬНЫХ УСТРОЙСТВ 264

Хамхоева Х.М., Абрамян Г.В.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации,
Российский государственный педагогический университет им. А. И. Герцена,
Санкт-Петербургский государственный институт психологии и социальной работы
ИНФОРМАЦИОННАЯ МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ НАВИГАЦИИ
МАРШРУТОВ ПОИСКА, ДИСТАНЦИОННОГО КОНСУЛЬТИРОВАНИЯ И ПОКУПОК
ТОВАРОВ НАРОДНОГО ПОТРЕБЛЕНИЯ 264

**ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИНАНСОВО-КРЕДИТНОЙ СФЕРЫ
И БИЗНЕСА..... 266**

Алмаметов Т.Г., Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ
АКТИВНОСТИ В ПРИЛОЖЕНИЯ ПОД ANDROID 266

Аминова Х.И., Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ГИБРИДНОЙ ОБЛАЧНОЙ ПЛАТФОРМЫ ДЛЯ ОРГАНИЗАЦИИ СОВРЕМЕННОЙ БАНКОВСКОЙ ИТ-ИНФРАСТРУКТУРЫ 267

Богатырев В.А., Паршутина С.А., Попцова Н.А.
Россия, Санкт-Петербург, Университет ИТМО
ИМИТАЦИОННАЯ МОДЕЛЬ СЕТИ С МНОГОПУТЕВОЙ РЕЗЕРВИРОВАННОЙ МАРШРУТИЗАЦИЕЙ 268

Богатырев В.А., Сластихин И.А.
Россия, Санкт-Петербург, Университет ИТМО
МЕЖМАШИННЫЙ ОБМЕН В РЕАЛЬНОМ ВРЕМЕНИ ЧЕРЕЗ РЕЗЕРВИРОВАННЫЕ КАНАЛЫ 269

Власова И.А.
Россия, Санкт-Петербург, Северо-Западный институт управления РАНХиГС
ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СУБЪЕКТОВ ВОЕННО-ТЕХНИЧЕСКОГО СОТРУДНИЧЕСТВА СО СТРАНАМИ СНГ 270

Гончаров В.В.
Россия, Санкт-Петербург, ООО «МЭС»
ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОЙ ПЕРЕПИСКЕ ПРЕДПРИЯТИЙ 270

Гончаров В.В.
Россия, Санкт-Петербург, ООО «МЭС»
ЗАДАЧИ РАЗВИТИЯ ВАЖНЕЙШИХ СИСТЕМ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ РОССИЙСКОЙ ЭКОНОМИКИ 271

Горенбургов М.А., Гончаров В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения, ООО «МЭС»
ЭВОЛЮЦИЯ БУХГАЛТЕРСКИХ ПРОГРАММ КАК ОБЪЕКТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ 272

Дзюбенко И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
МОДЕЛЬ ОЦЕНКИ ВРЕМЕННЫХ ХАРАКТЕРИСТИК ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СЕТИ IoT. 273

Корзина М.И., Антонов М.И., Корзин Ю.Н.
Россия, г. Архангельск, Северный (Арктический) федеральный университет имени М.В. Ломоносова, АТП «Панорама Retail»
РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДИАГНОСТИКИ КОНТРОЛЬНО-КАССОВОЙ ТЕХНИКИ 274

Сальникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ КУЛЬТУРНОЙ ПОЛИТИКИ ЧЕРЕЗ РАЗВИТИЕ ТРАНСЛЯЦИЙ В КИНОТЕТАРАХ 275

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 277

Бачиев Р.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЗАДАЧА РАСПОЗНАВАНИЯ СЛОЖНЫХ СИТУАЦИЙ НА ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ 277

Михайленко Е.И., Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»
РАЗВИТИЕ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ . 277

Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»
ГИБРИДНЫЙ ПРОТОКОЛ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ 278

Молокович И.А.
Россия, Санкт-Петербург, АО «НПО «Импульс»
МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ СЕТЯХ 279

Путилин А.Н., Шаптала В.С.
Россия, Санкт-Петербург, АО«НПО «Импульс»
АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ МАЛАГАБАРИТНОЙ СТАНЦИИ ТРОПОСФЕРНОЙ РАДИОСВЯЗИ 280

Стародубцев Ю.И., Чеснаков М.Н., Латушко Н.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
УПРАВЛЕНИЕ ПРОЦЕССАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР 281

Федосеев С.С.
Россия, Санкт-Петербург, АО «НПО «Импульс»
ОЦЕНКА ЭНЕРГЕТИЧЕСКИХ ХАРАКТЕРИСТИК РАДИОКАНАЛОВ ПУТЕМ СТАТИСТИЧЕСКОГО АНАЛИЗА РЕЗУЛЬТАТОВ ДОВЕДЕНИЯ СООБЩЕНИЙ 282

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ 283

Александров В.В., Зайцева А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
РАЗРАБОТКА ПОДХОДОВ К ОПРЕДЕЛЕНИЮ КУЛЬТУРОЛОГИЧЕСКИХ КАНОНОВ РАЗЛИЧНЫХ СОЦИАЛЬНЫХ ГРУПП НА ОСНОВЕ МЕТОДОВ АНАЛИТИЧЕСКОГО САМОРЕФЕРИРОВАНИЯ 283

Александров В.В., Кулешов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЦИФРОВАЯ ПРОГРАММИРУЕМАЯ ЭЛЕКТРОНИКА 284

Боруля П.Т, Фаткиева Р.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АСУТП КРИТИЧНЫХ ИНФРАСТРУКТУР 284

Бурлов В.Г. Мокеева Т.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
КОНЦЕПЦИЯ ПОДДЕРЖАНИЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ НА ОСНОВЕ ОБРАТНОЙ СВЯЗИ 285

Васильченко Д.С., Тындыкарь Л.Н., Берлова Н.М.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МОДЕЛИРОВАНИЕ ПРИ СОЗДАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ НА ПРЕДПРИЯТИИ 286

Демидова Н.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)
ОПТИМИЗАЦИЯ СОЗДАНИЯ ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ ДЛЯ ПРОИЗВОДСТВА ФЕРРИТОВ 287

Елисеева Ю.А., Ширяевская В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
ФУНКЦИОНАЛЬНО-СТОИМОСТНОЙ АНАЛИЗ КАК МЕТОД ОПТИМИЗАЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРЕДПРИЯТИИ СОЦИАЛЬНО-КУЛЬТУРНОЙ СФЕРЫ 287

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
О ПРЕДЕЛЬНЫХ ВОЗМОЖНОСТЯХ СООРУЖЕНИЙ, ЗАЩИЩАЮЩИХ САНКТ-ПЕТЕРБУРГ ОТ НАВОДНЕНИЙ, И НЕОБХОДТИМОСТИ РЕГУЛИРОВАТЬ СТОК РЕКИ НЕВЫ 288

Иванов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский морской технический университет,
МОНИТОРИНГ И ДИАГНОСТИКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ОБОРУДОВАНИЯ ГИДРОЭЛЕКТРОСТАНЦИЙ 288

Лукьянова Л.М., Заболотский В.П., Федорченко Л.Н.
Россия, Калининград, Калининградский государственный технический университет
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ДВЕ ЗАДАЧИ ФОРМИРОВАНИЯ СИСТЕМЫ ЦЕЛЕЙ: АНАЛИЗ И СИНТЕЗ ЦЕЛЕЙ 288

Лукьянова Л.М., Федорченко Л.Н.
Россия, Калининград, Калининградский государственный технический университет
Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ФОРМАЛИЗАЦИЯ ГРАММАТИК И ЯЗЫКОВ ПРОБЛЕМ И ЦЕЛЕЙ КОМПЛЕКСНЫХ СИСТЕМ ПРОИЗВОДСТВЕННОЙ СФЕРЫ 289

Ложкинс А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПОДХОД И ТЕХНОЛОГИИ К ОПЕРАТИВНОМУ ПЛАНИРОВАНИЮ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ 290

Михайлов Н.С.
Россия, Санкт-Петербург, АО «Равенство»
АРХИТЕКТУРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ 290

Петров В.А.
Россия, Санкт-Петербург, АО «Равенство»
ОПЕРАТИВНОЕ ПЛАНИРОВАНИЕ ПРОИЗВОДСТВА. 290

Рунёв Е.В., Сорокин Р.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербургский государственный университет
ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ В ЗАДАЧАХ С ОГРАНИЧЕНЫМИ РЕСУРСАМИ 291

Свиньин С.Ф., Зайнитдинов Х.Н., Хамдамов У.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Республика Узбекистан, г. Ташкент, Ташкентский университет информационных технологий
СПЛАЙН-ВЕЙВЛЕТЫ И ИХ ПРИМЕНЕНИЕ В ЗАДАЧАХ ВОССТАНОВЛЕНИЯ СИГНАЛОВ ПО ДИСКРЕТНЫМ ОТСЧЕТАМ 291

Цехановский В.В., Чертовской В.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
СИСТЕМНОЕ ПРИМЕНЕНИЕ ЗАДАЧИ СТАТИЧЕСКОГО ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ В АДАПТИВНОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ 292

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ 293

Бабуров В.И., Васильева Н.В., Иванцевич Н.В.
Россия, Санкт-Петербург, АО «ВНИИРА-Навигатор»
ИССЛЕДОВАНИЕ ТОЧНОСТИ НАВИГАЦИОННЫХ ОПРЕДЕЛЕНИЙ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПО СИСТЕМЕ ГЛОНАСС И ПСЕВДОСПУТНИКАМ В АРКТИЧЕСКОМ РЕГИОНЕ РОССИИ 293

Белоусов С.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО СПОПОСБА ОБРАБОТКИ ГРАФИКА ТОКА ПЕРЕВОДА СТРЕЛОЧНОГО ПЕРЕВОДНОГО УСТРОЙСТВА С ЭЛЕКТРОДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА ДЛЯ ДИАГНОСТИРОВАНИЯ НЕЙРОННОЙ СЕТЬЮ 293

Грошев В. А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ОСОБЕННОСТИ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ВЫСОКОСКОРОСТНЫХ МАГИСТРАЛЯХ МИРА 294

Ефанов Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ОБ ОСОБЕННОСТЯХ СИНТЕЗА ГЕНЕРАТОРОВ МОДИФИЦИРОВАННЫХ КОДОВ С СУММИРОВАНИЕМ С ПОСЛЕДОВАТЕЛЬНОСТЬЮ ВЕСОВЫХ КОЭФФИЦИЕНТОВ, ОБРАЗУЮЩЕЙ НАТУРАЛЬНЫЙ РЯД ЧИСЕЛ 295

Ефанов Д.В., Щагина В.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
КОД С СУММИРОВАНИЕМ ЕДИНИЧНЫХ РАЗРЯДОВ НА ОСНОВЕ ПРИНЦИПА ВЫДЕЛЕНИЯ ГРУПП РАЗРЯДОВ И ИХ КОНТРОЛЯ ПО МОДУЛЮ 4 295

Ефанов Д.В., Лыков А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
СОВЕРШЕНСТВОВАНИЕ СХЕМНЫХ РЕШЕНИЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА ЖЕЛЕЗНОДОРОЖНЫХ ПЕРЕЕЗДАХ ПРИ ОРГАНИЗАЦИИ ВЫСОКОСКОРОСТНОГО СООБЩЕНИЯ 296

Журавлева Л.М., Ивашевский М.Р., Григорук А.А., Ефимова Н.О.
Россия, г. Москва, Московский государственный университет путей сообщения Императора Николая II
ПОВЫШЕНИЕ ТЕХНИЧЕСКОГО УРОВНЯ БАЗОВЫХ ЭЛЕМЕНТОВ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ 297

Зозуля А.Р.
Россия, г. Петрозаводск, Петрозаводская дистанция сигнализации, централизации и блокировки Октябрьской дирекции инфраструктуры Октябрьской железной дороги
МОДИФИКАЦИЯ АЛГОРИТМА ВЫЯВЛЕНИЯ ПРЕДОТКАЗНЫХ СОСТОЯНИЙ В СИСТЕМЕ ТЕХНИЧЕСКОГО ДИАГНОСТИРОВАНИЯ И МОНИТОРИНГА УСТРОЙСТВ АВТОМАТИКИ НА ПОЛИГОНЕ ОКТЯБРЬСКОЙ ЖЕЛЕЗНОЙ ДОРОГИ 297

Исаева М.Ф., Глухарев М.Л.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ В ГЕТЕРОГЕННЫХ РАСПРЕДЕЛЁННЫХ ИСТОЧНИКАХ ДАННЫХ И ПРОБЛЕМЫ ЕЁ ОБЕСПЕЧЕНИЯ 298

Калинин В.М.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ИСПОЛЬЗОВАНИЕ СТОХАСТИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ ИНФОРМАЦИИ В МЕТОДАХ ОПТИМИЗАЦИИ 299

Киджи Д.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
КРАТКИЙ АНАЛИЗ И ОЦЕНКА РИСКОВ ПРИ ИСПОЛЬЗОВАНИИ ЭКНИС 300

Клименко С.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения императора Александра I
РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ ТРАНСПОРТНЫХ ПОТОКОВ 301

Кокурин И.М., Тимченко В.С.
Россия, Санкт-Петербург, Институт проблем транспорта им. Н.С. Соломенко РАН
КОМПЛЕКС ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ПЕРЕВОЗОК ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТИ ОБЕСПЕЧЕНИЯ ПРОПУСКНОЙ И ПРОВОЗНОЙ СПОСОБНОСТЕЙ ЖЕЛЕЗНОДОРОЖНОЙ ЛИНИИ, ОБСЛУЖИВАЮЩЕЙ МОРСКОЙ ПОРТ 302

Кушпиль И.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ЭКСПЛУАТАЦИОННО-ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ ПРИМЕНЕНИЯ СОЛНЕЧНОЙ ЭНЕРГИИ ДЛЯ ПИТАНИЯ АППАРАТУРЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ 303

Марков Д.С., Соколов В.Б., Соколов М.Б.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ОСОБЕННОСТИ СИНТЕЗА МОДЕЛИ ПОРЦИОННОГО ДИНАМИЧЕСКОГО МОДЕЛИРОВАНИЯ СЛОЖНЫХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ 304

Матушев А.А., Седых Д.В., Ушаков И.С.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
РАЗРАБОТКА ОБОБЩЕННОЙ МОДЕЛИ ПРИНЦИПИАЛЬНЫХ ЭЛЕКТРИЧЕСКИХ И МОНТАЖНЫХ СХЕМ ДЛЯ ЭКСПЕРТИЗЫ И ИНТЕЛЛЕКТУАЛЬНОЙ КОРРЕКТИРОВКИ 305

Ныркова А.П., Ныркова А.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ИСПОЛЬЗОВАНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ МАКСИМУМОВ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ СУДОХОДСТВА 305

Павлова Л.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРИМЕНЕНИЕ ПРОГРАММНОГО ПРОДУКТА ДЛЯ РАСЧЕТА ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ПРОЦЕССОВ ХРАНЕНИЯ И ПЕРЕРАБОТКИ РЕФРИЖЕРАТОРНЫХ КОНТЕЙНЕРНЫХ ГРУЗОВ..... 306

Пивоваров Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПОЛНОСТЬЮ САМОПРОВЕРЯЕМЫХ СТРУКТУР НА ОСНОВЕ РАВНОВЕСНОГО КОДА «1 ИЗ 4» 307

Плеханов П.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
РЕАЛИЗАЦИЯ КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ НА ОСНОВЕ ВОЗМОЖНОСТЕЙ БЕСПРОВОДНОЙ СВЯЗИ ПЯТОГО ПОКОЛЕНИЯ (5G) 308

Правдухина А.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
СИСТЕМЫ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ НА ОСНОВЕ КОДОВ С СУММИРОВАНИЕМ С ОДНИМ ВЗВЕШЕННЫМ РАЗРЯДОМ 309

Приходько А.М., Приходько В.М.
Украина, г. Днепр, Национальная металлургическая академия Украины
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МЕТОДЫ ПОВЫШЕНИЯ ПОКАЗАТЕЛЕЙ РАБОТЫ ДВИГАТЕЛЕЙ НА ВОДНОМ ТРАНСПОРТЕ 310

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АСИНХРОННЫХ ДВИГАТЕЛЕЙ ДЛЯ СУШКИ ИЗОЛЯЦИОННЫХ СИСТЕМ НА ВОДНОМ ТРАНСПОРТЕ..... 311

Приходько В.М., Приходько И.В., Лучкин В.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
АВТОМАТИЗАЦИЯ ОПРЕДЕЛЕНИЯ ТОКОВ АВАРИЙНЫХ ДУГОВЫХ КОРОТКИХ ЗАМЫКАНИЙ НА ВОДНОМ ТРАНСПОРТЕ 311

Приходько В.М., Приходько И.В., Игнатов Д.И.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ИНФОРМАЦИОННЫЙ АСПЕКТ ПРОБЛЕМЫ ЭНЕРГОСБЕРЕЖЕНИЯ НА ВОДНОМ ТРАНСПОРТЕ..... 312

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ТЕХНИКО-ЭКОНОМИЧЕСКИЙ АНАЛИЗ СУДОВЫХ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ С ПОЛУПРОВОДНИКОВЫМИ ПРЕОБРАЗОВАТЕЛЯМИ..... 313

Приходько В.М., Приходько И.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
КРИТЕРИЙ ОЦЕНКИ ПОТЕРЬ ПРИ РАСПРЕДЕЛЕНИИ ЭЛЕКТРОЭНЕРГИИ В СУДОВЫХ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМАХ..... 314

Ревера Г.М.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
СТЕГАНОГРАФИЯ НА ВОДНОМ ТРАНСПОРТЕ 315

Седых Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
МЕТОДЫ СВЕРКИ ЧЕРТЕЖЕЙ НАПОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ..... 316

Тришин Н.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ДОСТИЖЕНИЕ ОПТИМУМА РЕДУКЦИИ КОНЕЧНОГО АВТОМАТА С ТОЧКИ ЗРЕНИЯ ЭВРИСТИЧЕСКОГО ПОДХОДА АЛГОРИТМА STAMINA 317

Удалов В.С., Гаскаров В.Д
Россия, Санкт-Петербург, ФБУ «Администрация «Волго-Балт»
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ПОЛОЖЕНИЯ СУДНА В КАМЕРЕ ШЛЮЗА ПРИ ПОМОЩИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ЗА ПРОЦЕССОМ СУДОПРОПУСКА 318

Удалов В.С., Гаскаров В.Д.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ СТРУКТУРЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПО ИСТЕЧЕНИИ СРОКА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ПРОИЗВОДИТЕЛЯ 319

Хорошев В.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ЭЛЕКТРОННАЯ СИСТЕМА КОНТРОЛЯ БЕЗОПАСНОСТИ РАБОТНИКА НА ЖЕЛЕЗНОДОРОЖНЫХ ПУТЯХ 320

Черепанова М. Р.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
К ВОПРОСУ О СРАВНЕНИИ ХАРАКТЕРИСТИК СИСТЕМ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ, СИНТЕЗИРОВАННЫХ С ИСПОЛЬЗОВАНИЕМ КЛАССИЧЕСКИХ И ВЗВЕШЕННЫХ КОДОВ С СУММИРОВАНИЕМ 321

Чертовской В.Д.
Россия, С.-Петербург, ГУМРФ им. адм. С.О. Макарова
ВОПРОСЫ ПОСТРОЕНИЯ И РЕАЛИЗАЦИИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ 321

Чухонин В.М., Осадчий Г.В., Фомин Д.В.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ИСПОЛЬЗОВАНИЕ СВОЙСТВ САМОПРОВЕРЯЕМЫХ ПАРАФАЗНЫХ АВТОМАТОВ В СОЧЕТАНИИ СО СВОЙСТВАМИ МАЖОРИТАРНОЙ ФУНКЦИИ ПРИ ПРОГРАММНОЙ РЕАЛИЗАЦИИ 322

Яицкий И.А.
Россия, Санкт-Петербург, Петербургский государственный университет путей сообщения Императора Александра I
ПРОБЛЕМА УЧЕТА ТЕПЛОВЫДЕЛЕНИЯ ОТ РЕЛЕЙНЫХ И МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЭЛЕКТРИЧЕСКИХ ЦЕНТРАЛИЗАЦИЙ 323

Яшин М.Г., Пантелеев Р.А., Шарлай А.С., Фомин С.Н., Цуриков С.В.
Россия, Санкт-Петербург, Военный институт (Железнодорожных войск и военных сообщений) Военной академии материально-технического обеспечения
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ВОССТАНОВЛЕНИИ СТАНЦИОННЫХ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ 323

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУЧНЫХ ИССЛЕДОВАНИЯХ 325

Бусыгин А.Г., Коноплев А.С.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ 325

Верзун Н.А., Ипатов О.С., Колбанёв А.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОПТИМИЗАЦИЯ ПРОЦЕССА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕТЯХ БУДУЩЕГО ПО КРИТЕРИЮ ЭНЕРГОЭФФЕКТИВНОСТИ 326

Горбунова И.Б., Чибирёв С.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена
КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЭЛЕМЕНТОВ МУЗЫКАЛЬНОГО ТВОРЧЕСТВА 326

Евневич Е.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОПРЕДЕЛЕНИЕ ТЕНДЕНЦИЙ РАЗВИТИЯ КОГНИТИВНЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ АНАЛИЗА ПАТЕНТНОЙ ИНФОРМАЦИИ 327

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМЫ ПРОГНОЗИРОВАНИЯ КОСМИЧЕСКОЙ ПОГОДЫ И ПОЛЕТЫ НА МАРС 328

Ипатов О.С., Колбанёв М.О., Татарникова Т.М.
Россия, г. Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Санкт-Петербургский государственный университет аэрокосмического приборостроения
НОВЫЙ ВЗГЛЯД НА МОДЕЛЬ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ 328

Колоколов Д.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)
ПРОБЛЕМЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ХИМИИ И МАТЕРИАЛОВЕДЕНИИ 329

Кузнецова А.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПОПУЛЯРНЫЕ АЛГОРИТМЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ 329

Левшун Д.С., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СРАВНЕНИЕ ПОДХОДОВ К ПОСТРОЕНИЮ БАЗ ДАННЫХ ДЛЯ ОРГАНИЗАЦИИ ПОИСКА МАТЕРИАЛОВ В ЕДИНОМ ХРАНИЛИЩЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ ИЗ ПОЛЕВЫХ ЭТНОГРАФИЧЕСКИХ ЭКСПЕДИЦИЙ 330

Нечитайленко Р.А., Новопашин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРИНЦИПЫ ВЗАИМОДЕЙСТВИЯ ВЕБ-СЕРВИСОВ В РАМКАХ СЕРВИСНО-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ 331

Острейковский В.А., Демченко М.Л.
Россия, г. Сургут, Сургутский государственный университет
ТЕОРИЯ ФРАКТАЛОВ ДЛЯ ОЦЕНКИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ 332

Острейковский В.А., Муравьев И.И., Павлов А.С.
Россия, г. Сургут. Сургутский государственный университет, Сургут, ОАО «Сургутнефтегаз», ПУ «СургутАСУнефть»,
г. Обнинск, Обнинский институт атомной энергетики – филиал НИЯУ МИФИ
МОДЕЛИРОВАНИЕ СЛУЧАЙНЫХ ПРОЦЕССОВ В ЗАДАЧАХ ОЦЕНКИ ФАКТОРА ВРЕМЕНИ ТЕОРИИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ СИСТЕМ 332

Острейковский В.А., Шевченко Е.Н.
Россия, г. Сургут, Сургутский государственный университет
ОБРАТИМЫЕ И НЕОБРАТИМЫЕ ВО ВРЕМЕНИ ПРОЦЕССЫ В ТЕОРИИ ТЕХНОГЕННОГО РИСКА СЛОЖНЫХ СИСТЕМ 333

Христофоров М.В.
Россия, Санкт-Петербург, Университет ИТМО
СИСТЕМЫ ДЛЯ АВТОМАТИЗИРОВАННОГО СБОРА ДАННЫХ ИЗ ГЕТЕРОГЕННЫХ ИСТОЧНИКОВ В ОРГАНИЗАЦИИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ 333

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ 335

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена, Финансовый университет при Правительстве РФ, Санкт-Петербургский государственный институт психологии и социальной работы
МЕТОДОЛОГИЯ АНАЛИЗА, КЛАССИФИКАЦИИ И ТАКСОНОМИИ ЦЕЛЕЙ ОБУЧЕНИЯ ИНФОРМАТИКЕ И ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ В УСЛОВИЯХ ИНТЕРНАЦИОНАЛИЗАЦИИ ОБРАЗОВАНИЯ, ПОЛЯРИЗАЦИИ ЭКОНОМИЧЕСКИХ РЫНКОВ, РЕГИОНАЛЬНОЙ И ГЛОБАЛЬНОЙ МИГРАЦИИ ТРУДОВЫХ РЕСУРСОВ 335

Алексанова Л.В.
Россия, г. Новосибирск, Российский государственный педагогический университет им. А.И. Герцена
ВОЗМОЖНОСТИ И ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В ОБРАЗОВАНИИ 336

Бажукова Е.Н.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ИНФОРМАЦИОННАЯ КУЛЬТУРА КАК СРЕДСТВО ПРЕОДОЛЕНИЯ ФОРМАЛИЗМ ЗНАНИЙ ПЕДАГОГОВ-МУЗЫАНТОВ 337

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ» 338

Барышникова Н.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОРГАНИЗАЦИЯ ОБРАБОТКИ ЗАПРОСОВ ПОЛЬЗОВАТЕЛЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ЭЛЕКТРОННОГО ТЕСТИРОВАНИЯ НА ОСНОВЕ СЕМАНТИЧЕСКИХ СЕТЕЙ И ШАБЛОНОВ 339

Барышникова Н.Ю., Егоров А.Н., Крупенина Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ В РАМКАХ ИЗУЧЕНИЯ ЯЗЫКА ЗАПРОСОВ СРЕДЫ «1С: ПРЕДПРИЯТИЕ 8» 340

Белов Г.Г.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургская государственная консерватория имени Н.А. Римского-Корсакова
ОБРАЩЕНИЕ К КОМПЬЮТЕРНЫМ ТЕХНОЛОГИЯМ В МУЗЫКЕ - НЕИЗБЕЖНЫЙ ФАКТОР ВРЕМЕНИ: РАЗМЫШЛЕНИЯ КОМПОЗИТОРА 341

Бергер Н.А., Яцентковская Н.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Санкт-Петербургская государственная консерватория имени Н.А. Римского-Корсакова
ФУНДАМЕНТАЛИЗАЦИЯ МУЗЫКАЛЬНОГО ОБРАЗОВАНИЯ: ИНФОРМАЦИОННЫЙ ПОДХОД. 341

Верхолат А.М.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ИНФОРМАЦИОННО-ПРОГРАММНЫЙ КОМПЛЕКС ВЫЯВЛЕНИЯ ПЛАГИАТА В КУРСОВЫХ ПРОЕКТАХ ПО ТЕХНОЛОГИЯМ БАЗ ДАННЫХ 342

Воронов А.М., Криводонова Ю.Е.
Россия, Санкт-Петрубург, Российский государственный педагогический университет им. А.И. Герцена,
Екатеринбург, Уральский государственный педагогический университет
МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ ЛЮДЕЙ С НАРУШЕНИЕМ ЗРЕНИЯ 343

Гавронская Ю.Ю, Оксенчук В.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ВИРТУАЛЬНЫЕ ХИМИЧЕСКИЕ ЛАБОРАТОРИИ В ВУЗОВСКОМ ОБРАЗОВАНИИ 344

Говорова А.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ МУЗЫКЕ НОТНОЙ ГРАМОТЕ УЧАЩИХСЯ-ИНВАЛИДОВ ПО ЗРЕНИЮ 345

Голоскоков К.П., Чиркова М.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ПОРТФОЛИО СТУДЕНТА ВУЗА 346

Гончарова М.С.
Россия, Санкт-Петербург Российский государственный педагогический университет им. А.И. Герцена
МОБИЛЬНОЕ ОБУЧЕНИЕ В СИСТЕМЕ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГА-МУЗЫКАНТА..... 347

Графов А.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ..... 348

Давлетова К.Б.
Россия, Санкт-ПетербургЦентр творческого развития и гуманитарного образования детей «На Васильевском»
ОСНОВНЫЕ КОМПОНЕНТЫ СОВРЕМЕННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГА-МУЗЫКАНТА 348

Дмитриева Л.М., Батенькина О.В.
Россия, г. Омск, Омский государственный технический университет
РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЦЕНТР ДИАГНОСТИКИ УРОВНЯ РАЗВИТИЯ И КОРРЕКЦИОННОГО ОБУЧЕНИЯ ДЕТЕЙ ДОШКОЛЬНОГО ВОЗРАСТА С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ»..... 349

Дубенецкий В.А., Кузнецов А.Г., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОБЛЕМЫ АДАПТАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ БАКАЛАВРОВ И МАГИСТРОВ ПО НАПРАВЛЕНИЮ "ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ" К СОВРЕМЕННЫМ СТАНДАРТАМ CDIO 351

Ежгуров В.Н., Доброрадова В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ВНЕДРЕНИЕ И РАЗРАБОТКА СМС ИНФОРМИРОВАНИЯ В ВЫСШЕМ УЧЕБНОМ ЗАВЕДЕНИИ..... 352

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРАВОВОЙ АСПЕКТ ВНЕДРЕНИЯ В УНИВЕРСИТЕТЕ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ..... 352

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ВНЕДРЕНИЯ СИСТЕМЫ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ..... 353

Ежгуров В.Н.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ОБОСНОВАНИЕ ВНЕДРЕНИЯ В УНИВЕРСИТЕТЕ СИСТЕМЫ АУДИО И ВИДЕО ЗАПИСИ КОНТРОЛЬНЫХ ТОЧЕК ОБУЧЕНИЯ..... 354

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет
ПРЕДЛОЖЕНИЯ ПО ВНЕДРЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СОВМЕСТНОЙ РАБОТЫ С ДОКУМЕНТАМИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ..... 354

Жигадло Н.В., Елисеева Е.Н.
Россия, Санкт-Петербург, Гимназия № 652
ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ИНТЕРАКТИВНЫХ СРЕДСТВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ В УСЛОВИЯХ ПРЕЕМСТВЕННОСТИ ФГОС НОО 355

Журавлев А.Е.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
СПЕЦИАЛЬНЫЙ ФУНКЦИОНАЛ В ИНФОРМАЦИОННЫХ СИСТЕМАХ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ КОМПЕТЕНЦИЙ В КОНТЕКСТЕ АКТУАЛЬНЫХ ФГОС 356

Заболотная В.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ БАКАЛАВРОВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА 357

Игнатьев М.Б., Попов В.П., Аксенов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
НОВАЯ МАГИСТЕРСКАЯ ПРОГРАММА «КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ» 358

Камерис А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
РЕАЛИЗАЦИЯ КОНЦЕПЦИИ МУЗЫКАЛЬНО-КОМПЬЮТЕРНОГО ОБРАЗОВАНИЯ В СИСТЕМЕ ПОДГОТОВКИ ПЕДАГОГА-МУЗЫКАНТА 358

Касаткин В.В., Советов Б.Я.
Россия,Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНТЕГРАЦИЯ ОБРАЗОВАНИЯ, НАУКИ И ПРОМЫШЛЕННОСТИ КАК ОСНОВА РОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ ИТ-СПЕЦИАЛИСТОВ ПРИ МНОГОУРОВНЕВОЙ ПОДГОТОВКЕ 359

Касаткин В.В., Советов Б.Я., Яковлев С.А.
Россия,Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
АКТУАЛИЗАЦИЯ ПРИМЕРНЫХ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ НА ОСНОВЕ СОПРЯЖЕНИЯ ФГОС С ПРОФЕССИОНАЛЬНЫМИ СТАНДАРТАМИ 360

Касаткин В.В., Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 361

Каткова И.В., Павлова С.М.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ 362

Кибиткина Э.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
МЕТАМЕТОДИЧЕСКИЕ ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МУЛЬТИМЕДИА 363

Климов А.Н., Терехин Д.В., Чирушкин К.А
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРЕДПОСЫЛКИ И АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ УЧЕБНЫХ ТРЕНАЖЕРОВ В ПРОЦЕССЕ ПОДГОТОВКИ КАДРОВ И КОНТРОЛЯ НАВЫКОВ ПРИ ВЫПОЛНЕНИИ РАБОТ НА ВЫСОКОТЕХНОЛГИЧНОМ ОБОРУДОВАНИИ 364

Колоколова Л.П.
Россия, г. Стерлитамак, Стерлитамакский филиал Башкирского государственного университета
ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА ПРИ ИЗУЧЕНИИ КОРПУСНОЙ ЛИНГВИСТИКИ... 365

Комарова С.М.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена
ОБУЧЕНИЕ СТУДЕНТОВ КОМПЬЮТЕРНОМУ МОДЕЛИРОВАНИЮ НА ОСНОВЕ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ 366

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
СОЦИАЛЬНЫЕ СЕТИ И ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС 366

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС И ИКТ..... 368

Копыльцов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Смольный институт Российской академии образования
КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В СРЕДНЕМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАНИИ 369

Костюченко О.А.
Россия, Санкт-Петербург, Детская студия мультимедиа «M-Art» Санкт-Петербургского Центра творческого развития и гуманитарного образования детей «На Васильевском» Президентская библиотека имени Б.Н. Ельцина
МУЛЬТИМЕДИЙНОЕ ПРОЕКТИРОВАНИЕ В ДЕТСКОМ ОБРАЗОВАНИИ. МУЛЬТИМЕДИЙНЫЙ ФИЛЬМ «МЫ И КОСМОС» 370

Лаптев В.В., Баранова Е.В., Симонова И.В.
Россия, г. Москва, Российская академия образования
Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ХАРАКТЕРИСТИКА ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ДЛЯ НЕПРЕРЫВНОЙ ПОДГОТОВКИ УЧИТЕЛЕЙ ИНФОРМАТИКИ В ПЕДАГОГИЧЕСКОМ ВУЗЕ 371

Марченко Е.П.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена
МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ПОДГОТОВКЕ ПЕДАГОГА-МУЗЫКАНТА К ДУХОВНО-НРАВСТВЕННОМУ ВОСПИТАНИЮ МОЛОДЕЖИ В ШКОЛЕ ЦИФРОВОГО ВЕКА 371

Митрофанова А.В., Ковальногова Н.М., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
МЕТОДЫ АВТОМАТИЗИРОВАННОГО ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ПОСТРОЕНИЯ ИНДИВИДУАЛЬНОЙ ТРАЕКТОРИИ ОБУЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 372

Митрофанова А.В., Ковальногова Н.М., Соколов С.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРЕДПОСЫЛКИ СОЗДАНИЯ АВТОМАТИЗИРВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ОБУЧАЮЩЕГОСЯ ПРИ ПОСТРОЕНИИ ИНДИВИДУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ТРАЕКТОРИИ В РАМКАХ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ 373

Морозов С.А.
Россия, г. Курск, Курский музыкальный колледж-интернат слепых
РОЛЬ СОВРЕМЕННЫХ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ СТУДЕНТОВ – ИНВАЛИДОВ ПО ЗРЕНИЮ В СРЕДНИХ ПРОФЕССИОНАЛЬНЫХ МУЗЫКАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЯХ..... 374

Николаева Д.С.
Россия, Санкт-Петербург, Школа № 53 Приморского района Санкт-Петербурга,
Российский государственный педагогический университет им.А.И.Герцена
МЕЖДУНАРОДНЫЕ УЧЕБНЫЕ ПРОЕКТЫ В РАМКАХ КУРСА ИНФОРМАТИКИ И ИКТ В КОНТЕКСТЕ ИНКЛЮЗИВНОГО ОБРАЗОВАНИЯ 375

Носкова Т.Н., Павлова Т.Б., Тумалева Е.А. Яковлева О.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
СОЦИАЛЬНЫЕ МЕДИА КАК ФАКТОР ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ СПЕЦИАЛИСТА В ОБЛАСТИ ОБРАЗОВАНИЯ 375

Нымм В.Р., Пиотровская К.Р., Еремеева Ю.П., И.С. Макогон
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
СТАТИСТИЧЕСКИЕ МЕТОДЫ В КОМПЬЮТЕРНОЙ ЛИНГВОДИДАКТИКЕ 376

Обухова Е.Н.
Россия, г. Ростов-на-Дону, Донской государственный технический университет
АНАЛИЗ РАНЖИРОВАННОЙ ОЦЕНКИ ЗНАНИЙ ПО РЕЗУЛЬТАТАМ ФАКТОННОГО ТЕСТИРОВАНИЯ 377

Одинокая М.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет имени Петра Великого
КОНЦЕПЦИЯ РАЗРАБОТКИ ИНТЕРАКТИВНЫХ ЭЛЕКТРОННЫХ УЧЕБНИКОВ ВУЗа 378

Панкова А.А.
Россия, г. Воронеж, Детская школа искусств №7 городского округа г. Воронеж
РОЛЬ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В СТАНОВЛЕНИИ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ БУДУЩИХ УЧИТЕЛЕЙ МУЗЫКИ 379

Пелевин М.С., Богданов Т.Р.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ИТ НАПРАВЛЕНИЙ 380

Плотников К.Ю.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
Е-МУЗЫКА: ПОТЕНЦИАЛ ДЛЯ САМОРЕАЛИЗАЦИИ ШКОЛЬНИКА 381

Погодин А.В., Погодина Ю.А., Голомолзин Р.С.
Россия, г. Москва, Технологический университет
Санкт-Петербург, ООО «Центр образовательных проектов и консалтинга «РАДУГА»
ИНФОРМАЦИОННАЯ СРЕДА УЧЕБНЫХ УЧРЕЖДЕНИЙ И ЕЕ ИНТЕГРАЦИЯ С ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ 381

Попова Е.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
МЕТОД ЭКСПЕРТНОЙ ОЦЕНКИ ДЛЯ ФОРМИРОВАНИЯ ИЗМЕРЕНИЙ ПРИ МНОГОКРИТЕРИАЛЬНОМ ВЫБОРЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ 382

Смолина Е.В.
Россия, Санкт-Петербург, Президентская библиотеки имени Б.Н. Ельцина
ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ РЕСУРСОВ НАЦИОНАЛЬНЫХ БИБЛИОТЕК В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ (НА ПРИМЕРЕ РАБОТЫ С ЧИТАТЕЛЯМИ БИБЛИОТЕКИ КОНГРЕССА) 383

Советов Б.Я., Касаткин В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ФУНДАМЕНТАЛИЗАЦИЯ И ПРОФЕССИОНАЛЬНАЯ ОРИЕНТАЦИЯ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 384

Советов Б.Я., Касаткин В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербургский институт информатики и автоматизации Российской академии наук
РОЛЬ АСПИРАНТУРЫ КАК ТРЕТЬЕЙ СТУПЕНИ ВЫСШЕГО ОБРАЗОВАНИЯ ИТ-СПЕЦИАЛИСТОВ 385

Тен Э.С.
Россия, Санкт-Петербург, Академическая гимназия № 56
МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ НА УРОКАХ МУЗЫКИ В ОБЩЕОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ: ИЗ ОПЫТА РАБОТЫ В АКАДЕМИЧЕСКОЙ ГИМНАЗИИ № 56 г. САНКТ-ПЕТЕРБУРГА..... 386

Титова Ю.Ф.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ОБ ОСОБЕННОСТЯХ ТРУДА ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ..... 387

Товпич И.О.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРЕПОДАВАНИИ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН 388

Устюгова Т.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
СЕТЕВЫЕ СЕРВИСЫ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ В ПОДГОТОВКЕ БАКАЛАВРОВ ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ..... 388

Фатьянова Е.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ПЕРСПЕКТИВЫ ОБУЧЕНИЯ ИГРЕ НА СИНТЕЗАТОРЕ В СИСТЕМЕ СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ 389

Хомутская Н.Ю.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена, Детская школа искусств Красносельского района
ИМПРОВИЗАЦИЯ НА ЭЛЕКТРОННЫХ МУЗЫКАЛЬНЫХ ИНСТРУМЕНТАХ..... 390

Черний В. Н.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ИНТЕРАКТИВНЫЕ МЕТОДЫ ОБУЧЕНИЯ СТУДЕНТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 390

Чёрная М.Ю.
Россия, Санкт -Петербург, Смольный институт Российской академии образования
ФОРМИРОВАНИЕ НОВОЙ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ МЫШЛЕНИЯ СОВРЕМЕННОГО МУЗЫКАНТА 391

Чистякова Т.Б., Новожилова И.В., Полосин А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный технологический институт (технический университет)
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННОГО ОБУЧЕНИЯ СПЕЦИАЛИСТОВ МЕЖДУНАРОДНЫХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ 392

Шалаева Е.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ВОЗМОЖНОСТИ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В РАЗВИТИ ОБЩЕКУЛЬТУРНЫХ КОМПЕТЕНЦИЙ СТУДЕНТОВ – БУДУЩИХ ПЕДАГОГОВ..... 393

Шутов И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский техникум железнодорожного транспорта
СЕТЕВАЯ ОБРАЗОВАТЕЛЬНАЯ СРЕДА КАК СРЕДСТВО ФОРМИРОВАНИЯ КОРПОРАТИВНЫХ КОМПЕТЕНЦИЙ..... 393

Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННЫЙ СЦЕНАРИЙ ПРОИЗВОДСТВЕННЫХ ЗАДАЧ В ПРОФЕССИОНАЛЬНОМ ОБУЧЕНИИ СТУДЕНТОВ 394

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
АВАНГАРД В ИСКУССТВЕ – ПРАКТИЧЕСКОЕ ИЛЛЮСТРИРОВАНИЕ НЕПРОИЗВОЛЬНОГО ВНИМАНИЯ 395

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
РЕАЛИЗМ В ИСКУССТВЕ – ПРАКТИЧЕСКОЕ ИЛЛЮСТРИРОВАНИЕ ПРОИЗВОЛЬНОГО ВНИМАНИЯ. РЕАЛИЗМ КАК СТАДИЯ ГОТОВОЙ ХУДОЖЕСТВЕННОЙ ФОРМЫ. 396

Ясинская О.Л.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
МУЗЫКАЛЬНОЕ ТВОРЧЕСТВО НА БАЗЕ DIGITAL AUDIO WORKSTATION ABLETON LIVE (ОСНОВНЫЕ ВОЗМОЖНОСТИ ДЛЯ СИСТЕМЫ СОВРЕМЕННОГО МУЗЫКАЛЬНОГО ОБРАЗОВАНИЯ) 397

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ И ЗДРАВООХРАНЕНИИ 398

Бланк М.А., Бланк О.А., Дюк В.А.
Россия, Санкт-Петербург, Российский научный центр радиологии и хирургических технологий Министерства здравоохранения Российской Федерации,
Санкт-Петербургский институт информатики и автоматизации РАН
ОПЫТ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ DATA MINING ДЛЯ ВЫЯВЛЕНИЯ ФАКТОРОВ, ВЛИЯЮЩИХ НА ВЫРАЖЕННОСТЬ ПОСТЛУЧЕВОЙ ГЕМОДЕПРЕССИИ 398

Гайсин В.А., Виноградова Т. В., Кулинкин Б. С., Никонорова М. Л., Тишков А. В., Яицкий А.Н.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
ПРИМЕНЕНИЕ ПОЛИЛИНГВАЛЬНЫХ ПОСОБИЙ ПРИ ОБУЧЕНИИ ИНОСТРАННЫХ УЧАЩИХСЯ 399

Денисова Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ВЛИЯНИЕ СЛЕЖЕНИЯ В СЕТИ ИНТЕРНЕТ НА ПСИХОФИЗИОЛОГИЧЕСКОЕ БЛАГОПОЛУЧИЕ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ 400

Жвалевский О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОД АНАЛИЗА ФРАКТАЛЬНОЙ ДИНАМИКИ И ЕГО ПРИЛОЖЕНИЕ К ОБРАБОТКЕ ТЕНЗОТРЕМОРОГРАММ 401

Игнатьев М.Б., Сурженко Д.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Институт эволюционной физиологии и биохимии им.Сеченова РАН
МОДЕЛИРОВАНИЕ ОРГАНИЗМА ДЛЯ УМЕНЬШЕНИЯ ВРАЧЕБНЫХ ОШИБОК 402

Никонорова М.Л., Юрьева О.А.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
СПИРОМЕТРИЧЕСКОЕ И БРОНХОЛИТИЧЕСКОЕ ИССЛЕДОВАНИЯ В СРЕДЕ БД ACCESS 402

Никонорова М.Л., Юрьева О.А., Тишков А.В.
Россия, Санкт-Петербург, Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
АНАЛИТИЧЕСКАЯ ВИЗУАЛИЗАЦИЯ СТАНДАРТОВ СПИРОМЕТРИИ 403

Попов А.И.
Россия, г. Архангельск, Северный (Арктический) федеральный университет имени М.В. Ломоносова, Высшая школа информационных технологий и автоматизированных систем, лаборатория информатизации прикладных исследований
О СОСТОЯНИИ ИССЛЕДОВАНИЙ В ОБЛАСТИ ЭЛЕКТРОГАСТРОЭНТЕРОГРАФИИ В СЕВЕРНОМ (АРКТИЧЕСКОМ) ФЕДЕРАЛЬНОМ УНИВЕРСИТЕТЕ НА 2016 ГОД 404

Сухов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СОВРЕМЕННЫЕ СРЕДСТВА ПО КОНТРОЛЮ БЕЗОПАСНОСТИ ЛЕКАРСТВЕННЫХ СРЕДСТВ ОНЛАЙН СИСТЕМА ФАРМАКАНАДЗОР 405

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ 407

Алексеев А.А., Груздев В.Н., Кузнецов А.Ю., Шилин Б.В.
Россия, Санкт-Петербург, Санкт-Петербургский центр экологической безопасности РАН, Университет ИТМО
СРАВНЕНИЕ ВИДЕОСПЕКТРОМЕТРОВ ВИДИМОГО-БЛИЖНЕГО ИНФРАКРАСНОГО ДИАПАЗОНА С РАЗЛИЧНЫМИ ТИПАМИ ПОЛИХРОМАТОРОВ 407

Алексеев В.В., Орлова Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИЗМЕРЕНИЯ В ЭКОЛОГИИ. ОБЕСПЕЧЕНИЕ ЕДИНСТВА ИЗМЕРЕНИЙ ПРИ ФОРМИРОВАНИИ ОЦЕНОК СОСТОЯНИЯ ПРИРОДНЫХ ОБЪЕКТОВ 407

Афанасьев В.П., Васильченко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПРОВЕДЕНИЯ МОНИТОРИНГА АВТОНОМНОЙ СОЛНЕЧНОЙ ЭЛЕКТРОСТАНЦИИ СПБГЭТУ 408

Биненко В.И.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН
ЭКОЛОГИЧЕСКИЙ ОТКЛИК НА ИЗМЕНЧИВОСТЬ КЛИМАТА ПРИГРАНИЧНЫХ РЕГИОНОВ ЛЕНИНГРАДСКОЙ ОБЛАСТИ РФ, ЭСТОНИИ И ФИНЛЯНДИИ 409

Бузников А.А.
Россия. Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОЛЯРИЗАЦИЯ ОТРАЖЕННОГО СОЛНЕЧНОГО ИЗЛУЧЕНИЯ – ИСТОЧНИК ИНФОРМАЦИИ ОБ ЭКРЛОГИЧЕСКОМ СОСТОЯНИИ ПРИРОДНЫХ ОБЪЕКТОВ 409

Викторов С.В., Спиридонова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН
«ЭСТЕТИЧЕСКИЙ УЩЕРБ» КАК ЭКОЛОГИЧЕСКИЙ ФАКТОР 410

Викторов С.В., Спиридонова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности РАН
ОБЪЕКТ «ПРОШЛОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА» В ЦЕНТРЕ САНКТ-ПЕТЕРБУРГА 411

Воробьев Е.Н., Туленков Н.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИСПОЛЬЗОВАНИЕ ПАССИВНОГО КОГЕРЕНТНОГО ЛОКАЦИОННОГО КОМПЛЕКСА В ОРНИТОЛОГИИ 411

Горохов В.Л., Бузников А.А., Витковский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Университет ИТМО
ОБЪЕКТИВАЦИЯ КОГНИТИВНЫХ ОБРАЗОВ И ИХ ВНЕДРЕНИЕ В СРЕДУ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ ДЛЯ ЭКОЛОГИЧЕСКОГО И ТЕХНОСФЕРНОГО МОНИТОРИНГА 412

Горохов В.Л., Маяков А.Н., Бузников А.А., Витковский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Университет ИТМО
НЕПАРАМЕТРИЧЕСКОЕ ОЦЕНИВАНИЕ АНОМАЛИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДАХ И ИХ КОГНИТИВНАЯ ИНТЕГРАЦИЯ 412

Горяинов В.С., Черноок В.И., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), АО «Гипрорыбфлот»
ИДЕНТИФИКАЦИЯ ГИДРОБИОНТОВ ПО ДАННЫМ ЛИДАРНОГО ЗОНДИРОВАНИЯ 413

Гринь С.С., Кустов Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
РАЗРАБОТКА АППАРАТНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОГО КОМПЛЕКСА КОНТРОЛЯ БИОТЕСТОВЫХ РЕАКЦИЙ 413

Доронин А.П., Петроченко В.М., Козлова Н.А., Шмалько С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОЧИЩЕНИЕ ВОЗДУШНЫХ БАССЕЙНОВ КРУПНЫХ ГОРОДОВ ОТ ЗАГРЯЗНЯЮЩИХ ПРИМЕСЕЙ ПУТЕМ ИНТЕНСИФИЦИРОВАНИЯ ОСАДКОВ..... 414

Дюфур М.С. Игнатьев М.Б., Катермина Т.С., Ненашев В.А.
Россия, *Санкт-Петербургский государственный университет, Санкт-Петербургский государственный университет аэрокосмического приборостроения,
г. Нижневартовск Нижневартовский государственный университет
ПРОБЛЕМА ПРОГНОЗИРОВАНИЯ ЛИТОСФЕРНОЙ ПОГОДЫ 414

Елизаров В.В., Конопелько Л.А., Гришканич А.С., Жевлаков А.П., Кащеев С.В.
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
Всероссийский научно-исследовательский институт метрологии имени Д.И.Менделеева
КАЛИБРОВКА РАМАНОВСКОГО ЛИДАРА С УЛЬТРАСПЕКТРАЛЬНЫМ РАЗРЕШЕНИЕМ 415

Захаров И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ВЫЯВЛЕННЫЕ СВОЙСТВА ТЕСТ-ОБЪЕКТОВ, ИСПОЛЬЗУЕМЫХ В АППАРАТУРНОМ МИКРОБИОТЕСТИРОВАНИИ 415

Казанцева А.Г., Завгородний А.В., Величко А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДОВ БИОТЕСТИРОВАНИЯ..... 416

Каткова И.В., Павлова С.М.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ 417

Летучий Ю.А., Новиков А.В., Тимощук А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МЕТОДИЧЕСКИЙ ПОДХОД К ОБРАЩЕНИЮ С ИСТОРИЧЕСКИМИ ЗАГРЯЗНЕНИЯМИ В АРКТИКЕ 418

Мелентьев В.В., Черноок В.И., Ковалев Г.А., Мелентьев А.В., Смирнова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, АО «НИИ и ПКИ по развитиюи эксплуатации флота»
АО «Гипрорыбфлот»
ИСПОЛЬЗОВАНИЕ ГИС ДЛЯ ВСЕПОГОДНОЙ ДИСТАНЦИОННОЙ РСА ДИАГНОСТИКИ МОРСКИХ АКВАТОРИЙ КАК СРЕДЫ ОБИТАНИЯ ЛЕДОВЫХ ФОРМ МОРСКИХ МЛЕКОПИТАЮЩИХ (НА ПРИМЕРЕ ЛАПТЕВОМОРСКОГО МОРЖА)..... 418

Рузанкина Ю.С., Васильев О.С., Парфенов В.А.
Россия, Санкт-Петербург, Университет ИТМО, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ТЕХНОЛОГИЯ ПОВЫШЕНИЯ КОРРОЗИОННОЙ СТОЙКОСТИ СТАЛИ МЕТОДАМИ ФОТОНИКИ 419

Смирнов Л.В., Гришканич А.С., Елизаров В.В., Кащеев С.В.
Россия, Санкт-Петербург, Университет ИТМО
ОСНОВНЫЕ ПОДХОДЫ К РАЗРАБОТКЕ ЛИДАРА ДЛЯ МОНИТОРИНГА ПОВЕРХНОСТИ МАРСА..... 420

Хафизов Н. Ф., Гришканич А.С., Рузанкина Ю.С.
Россия, Санкт-Петербург, Университет ИТМО
ЛАЗЕРНОЕ ОБЕЗЗАРАЖИВАНИЕ ВОДЫ..... 420

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ..... 421

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
ПРИНЦИП 80/20 И ЕГО РАЗВИТИЕ ДЛЯ СМЕЩЕННЫХ ОДНОРОДНЫХ ПРОЦЕССОВ 421

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
МОДЕЛЬ ОЦЕНКИ КАЧЕСТВА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ..... 422

Алексеев А.В., Воробьев В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, Санкт-Петербургский институт автоматизации и информатизации РАН
20 ЛЕТ КОНЦЕПТУАЛЬНОГО И ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ ПРОБЛЕМ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА 423

Алексеев А.В., Левадный И.В., Мусатенко Р.И., Смольников А.В., Сус Г.Н., Ушакова Н.П.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, АО «Концерн «НПО «Аврора»
ТЕХНОЛОГИЯ И ПРОГРАММНЫЙ КОМПЛЕКС СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ СУДОВОДИТЕЛЯ В СЕТЕВОМ ИСПОЛНЕНИИ (ТиПК «СПРУ-С»)..... 425

Алексеев А.В., Карпов А.Е., Мусатенко Р.И., Потехин В.С., Худобородов Е.Ф.
Россия, Санкт-Петербург, Военный учебно-научный центр ВМФ «Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова»
ОТ МОНИТОРИНГА ДАННЫХ К МОНИТОРИНГУ ПРОЦЕССОВ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ . 426

Поляничко В.В., Алексеев А.В.
Россия, Санкт-Петербург, ООО «ЦНИиР «Кристалл», НП «ИАП БЖКС»
КОНЦЕПЦИЯ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО МОНИТОРИНГА И ПРОЦЕССНОГО УПРАВЛЕНИЯ СТРУКТУРОЙ И КАЧЕСТВОМ ЖИЗНЕННОГО ЦИКЛА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ..... 427

Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, АО «Концерн «НПО «Аврора»
РАЗВИТИЕ МЕТОДОЛОГИИ ОМКАР И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ РАЗВИТИЕМ КРИТИЧЕСКИХ МОРСКИХ ОБЪЕКТОВ 428

Алексеев А.В., Согонов С.А., Равин А.А., Хруцкий О.В., Мусатенко Р.И., Потехин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, Военный учебно-научный центр ВМФ «Военно-морская академия», Санкт-Петербургский университет МВД России
МЕТОД ОЦЕНКИ КОМПЕТЕНТНОСТИ И ПОДГОТОВЛЕННОСТИ ЭКИПАЖА СУДНА..... 429

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, ГУМРФ имени адм. С.О. Макарова
ПРИНЦИПЫ И ЭТАПЫ ЭРГОНОМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОЕКТИРОВАНИЯ АРМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ..... 430

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, ГУМРФ имени адм. С.О. Макарова
ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЛИКА ИНТЕГРИРОВАННОЙ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ..... 432

Баркова Н.А., Грищенко Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИОННОЙ ДИАГНОСТИКИ ПЛАНЕТАРНЫХ РЕДУКТОРОВ НА МОРСКОМ ТРАНСПОРТЕ 433

Белячков С.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
УГРОЗЫ "ИНТЕРНЕТА ВЕЩЕЙ» 434

Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Согонов С.А., Ушакова Н.П., Петров А.А., Кузьмина С.Д., Поленин В.И., Соловьев С.Н., Москаленко В.А., Мусатенко Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна, Санкт-Петербургский государственный морской технический университет, АО «Концерн «НПО «Аврора», Центральный научно-исследовательский и проектно-конструкторский институт морского флота, Институт проблем управления РАН, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: ВТОРОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ 435

Бронников А.А
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ ТЕХНОЛОГИИ ШИФРОВАНИЯ WEP ДЛЯ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ 436

Гоманцов А.А., Горбачев В.А.
Россия, Санкт-Петербург, АО Центральное конструкторское бюро морской техники «Рубин», Военно-морской политехнический институт, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
К ВОПРОСУ О СИСТЕМНОЙ БЕЗОПАСНОСТИ СУДОВЫХ ЭНЕРГЕТИЧЕСКИХ КОМПЛЕКСОВ 437

Горбенко Е.А., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ МЕР ПО ПРЕДОТВРАЩЕНИЮ ИСПОЛЬЗОВАНИЯ SQL-ИНЪЕКЦИЙ В ИНФОРМАЦИОННЫХ РЕСУРСАХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 438

Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ИЗМЕНЕНИЕ СТРАТЕГИИ УПРАВЛЕНИЯ РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ ПРЕДПРИЯТИЯ МОРСКОЙ ИНФРАСТРУКТУРЫ 439

Каганский М.А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
КРИТИЧНОСТЬ ВЛИЯНИЯ СУБЪЕКТИВНЫХ СВОЙСТВ ОПЕРАТОРОВ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ ВМФ НА КАЧЕСТВО И РЕЗУЛЬТАТЫ УПРАВЛЕНИЯ 440

Кальбфляйш В. А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ЛИЧНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОСВЕДОМЛЕННОСТЬ ОБ ОКРУЖАЮЩИХ УГРОЗАХ 441

Калюта Н.Г.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
МЕТОДИКА ОЦЕНКИ ЖИВУЧЕСТИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЯ ПРИ БОЕВЫХ И АВАРИЙНЫХ ПОВРЕЖДЕНИЯХ 442

Карпов А.Е., Алексеев А.В., Худобородов Е.Ф.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
АКТУАЛЬНОСТЬ КВАЛИМЕТРИЧЕСКОЙ ОЦЕНКИ ПРЕВОСХОДСТВА ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА СЛОЖНЫХ ЭРГАТИЧЕСКИХ СИСТЕМ 443

Карпов А.Е., Алексеев А.В., Худобородов Е.Ф.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ПРИНЦИПЫ И БАЗОВЫЕ КРИТЕРИИ ОЦЕНКИ ПРЕВОСХОДСТВА ИНФРОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА СЛОЖНЫХ ЭРГАТИЧЕСКИХ КОМПЛЕКСОВ 444

Коваленко Д.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ИНФОРМАЦИОННАЯ ПОДДЕРЖКА КОМАНДИРА АВАРИЙНОЙ ПАРТИИ ПРИ ПОДГОТЛОВКЕ К БОРЬБЕ ЗА ЖИВУЧЕСТЬ И ЕЁ ВЕДЕНИИ 445

Леберянский А.П.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ОБЩИЕ КРИТЕРИИ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ КОРАБЛЯ 446

Максимова М.А., Петраков С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет, ООО «Фарадей инжиниринг»
СОВРЕМЕННЫЙ ПОДХОД К ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ КОТЕЛЬНЫХ УСТАНОВОК 446

Мозокин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СЕРВИСЫ, ТЕХНОЛОГИИ, УЯЗВИМОСТИ, УГРОЗЫ И ЗАЩИТА BLUETOOTH 447

Мокин С.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ОРГАНИЗАЦИЯ ПОДГОТОВКИ АВАРИЙНЫХ ПАРТИЙ ГЭУ ПЛА 448

Москаленко В. А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ИНФОМАЦИОННАЯ ПОДДЕРЖКА КОМАНДИРА ПОДВОДНОЙ ЛОДКИ ПРИ БОРЬБЕ С ПОЖАРАМИ НА ПЛ 449

Никитин А.Г.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ОСНОВНЫЕ НЕДОСТАТКИ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ СОВРЕМЕННЫХ КОРАБЛЕЙ ВМФ 450

Панфилов М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ МЕТОДОВ ПРИМЕНЕНИЯ SQL-ИНЪЕКЦИЙ И МЕР ПО ИХ ПРЕДОТВРАЩЕНИЮ 451

Поленин В.И., Можаева И.А., Потехин А.А., Сущенков Д.А.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»,
ООО НТЦ «Севзапмонтажавтоматика»
СОВЕРШЕНСТВОВАНИЕ ПРОГРАММНЫХ КОМПЛЕКСОВ АВТОМАТИЗИРОВАННОГО СТРУКТУРНОГО МОДЕЛИРОВАНИЯ С ПРИМЕНЕНИЕМ ОЛВМ ПО ВЕРОЯТНОСТНОЙ ОЦЕНКЕ ТЕКУЩЕЙ И ИТОГОВОЙ УСТОЙЧИВОСТИ БОЕВЫХ И ТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПОРАЖАЮЩИХ ФАКТОРОВ 452

Разживин Н.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
УЧЕБНО – ТРЕНАЖЕРНЫЙ КОМПЛЕКС ЦЕНТРА ОСВОЕНИЯ ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА 453

Рябцев М.Д.
Россия, Санкт-Петербург , ГУМРФ им. адм. С.О. Макарова
ИСТОРИЯ РАЗВИТИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПЕРЕВОЗКАМИ И РАБОТОЙ ФЛОТА В РОССИЙСКОЙ АРКТИКЕ 454

Салащенко А.И.
Россия, Санкт-Петербург, ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В ЗАДАЧАХ ЛОКАЛИЗАЦИИ АВАРИЙНЫХ СИТУАЦИЙ 454

Свиньин С.Ф., Алексеев А.В., Попов А.И., Федорченко Л.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный морской технический университет,
Северный (Арктический) федеральный университет имени М.В. Ломоносова
ТЕОРИЯ ИНФОРМАЦИИ: ОТ ТЕОРЕМЫ УКШ К ТЕОРИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ 457

Согонов С.А., Алексеев А.В., Тюрин И.С., Разживин Н.С., Жуланова Д.Н., Филиппова А.С., Шитикова К.А., Кальбфляш В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРЕДЛОЖЕНИЕ ПО СОЗДАНИЮ ПОЛИГОНА СЕТЕВОГО МЕЖВУЗОВСКОГО ВЗАИМОДЕЙСТВИЯ И МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА 458

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ЦОТИП В ВАРИАНТЕ "СПРУ-ИБ" 459

Удодова Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРИМЕНЕНИЕ ОБОБЩЕННОГО МЕТОДА КВАЛИМЕТРИЧЕСКОГО АНАЛИЗА ПРИ ФОРМИРОВАНИИ СТРАТЕГИИ РАЗВИТИЯ ПРЕДПРИЯТИЯ 460

Ушакова Н.П., Сус Г.Н., Алексеев А.В., Голубев И.Г, Москаленко В.А.
Россия, Санкт-Петербург, АО «Концерн «НПО «Аврора», Институт автоматизации процессов борьбы за живучесть корабля, судна
СИСТЕМНЫЕ ТРЕБОВАНИЯ И РАНЖИРОВАНИЕ КАЧЕСТВА ВАРИАНТОВ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ БЖКС 461

Ушакова Н.П., Москаленко В.А.
Россия, Санкт-Петербург, АО «Концерн «НПО «Аврора», ВУНЦ ВМФ «ВМА им. Н.Г. Кузнецова»
МОДЕЛЬ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА СОВРЕМЕННЫХ КОРАБЛЕЙ 462

Чернышев Д.Д., Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ ФИШИНГОВЫХ И АНТИФИШИНГОВЫХ ТЕХНОЛОГИЙ 464

Филиппова А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
К ВОПРОСУ О БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ МОРСКИМИ ОБЪЕКТАМИ 464

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕТЕОРОЛОГИИ АРКТИЧЕСКОГО РЕГИОНА 466

Антонов К.В., Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ОРГАНИЗАЦИЯ ПОДГОТОВКИ IT-СПЕЦИАЛИСТОВ ОСНОВАМ ЭКОЛОГИЧЕСКОЙ КУЛЬТУРЫ В АРКТИЧЕСКОМ РЕГИОНЕ 466

Антонов К.В., Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ В АРКТИЧЕСКОМ РЕГИОНЕ 467

Бабкин Ю.А., Фёдоров А.В.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи
РАЗРАБОТКА КОМПЛЕКСА АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ИЗМЕРЕНИЙ И КОНТРОЛЯ ЛИНЕЙНОГО ТРАКТА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ МАГИСТРАЛЬНО-РАСПРЕДЕЛЕННОГО ТИПА С КОММУТАЦИЕЙ ОПТИЧЕСКИХ КАНАЛОВ СВЯЗИ... 468

Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ОСОБЕННОСТИ «ГИБРИДНЫХ ВОЙН» В АРКТИЧЕСКОМ РЕГИОНЕ 471

Митько А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРИМЕНЕНИЕ ДИФФУЗНЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В АРКТИЧЕСКОМ РЕГИОНЕ..... 471

Митько В.Б.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи
СТРАТЕГИЧЕСКОЕ ЗНАЧЕНИЕ ФОРМИРОВАНИЯ ЕДИНОЙ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ АРКТИЧЕСКИХ РЕГИОНОВ 473

Митько В.Б., Минина М.В.
Россия, Санкт-Петербург, Ленинградское отделение Центрального научно-исследовательского института связи, Арктическая общественная академия наук
СОЗДАНИЕ ИННОВАЦИОННОГО ЦЕНТРА АРКТИЧЕСКИХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЛО ЦНИИС 474

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИЗДАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ, ПОЛИГРАФИИ И ДИЗАЙНЕ 476

Архипов П.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна
АНАЛИЗ ЭФФЕКТИВНОСТИ ИНТЕРНЕТ-КАНАЛОВ ПРИВЛЕЧЕНИЯ ТРАФИКА 477

Галимова Е.Ю.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
АНАЛИЗ ПОДХОДА К ТЕСТИРОВАНИЮ ПРОГРАММНОЙ СИСТЕМЫ НА БАЗЕ РЕШЕНИЯ МНОГОКРИТЕРИАЛЬНОЙ ЗАДАЧИ 477

Горина Е.В., Иващенко Д.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РАСПРЕДЕЛЕННЫХ ПОЛИГРАФИЧЕСКИХ СИСТЕМАХ 478

Горина Е.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОМОЩИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ..... 478

Горлицкая С.И., Вострых А.И., Доценко А.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
СОЗДАНИЕ ИНТЕРАКТИВНЫХ ИНСТАЛЛЯЦИЙ НА ОСНОВЕ КНИЖНЫХ ИЛЛЮСТРАЦИЙ..... 479

Груздева И.Г., Дмитрук В.В., Шелохова Е.Н.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ВЛИЯНИЕ ТЕХНОЛОГИЙ «HD_FLEXO» И «DIGI FLOW» НА КАЧЕСТВО ПЕЧАТИ..... 480

Груздева И.Г, Кудрин Ю.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
РАЗРАБОТКА СПЕЦИАЛЬНЫХ КРАСОЧНЫХ СОСТАВОВ НА ОСНОВЕ НЕОРГАНИЧЕСКИХ ЛЮМИНОФОРОВ ХАЛЬКОГЕНИДНОЙ ГРУППЫ ДЛЯ ЗАЩИТЫ УПАКОВОЧНОЙ ПРОДУКЦИИ ОТ ФАЛЬСИФИКАЦИИ 480

Гнатюк С.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна, Санкт-Петербургский государственный институт кино и телевидения
ОЦЕНКА ВЛИЯНИЯ ГЕОМЕТРИЧЕСКИХ И СОРБЦИОННО – АДГЕЗИОННЫХ СВОЙСТВ ЗАПЕЧАТЫВАЕМЫХ МАТЕРИАЛОВ НА КАЧЕСТВО РЕПРОДУКЦИИ НА ОСНОВЕ РЕЗУЛЬТАТОВ МАТЕМАТИЧЕСКОГО ОПИСАНИЯ СВЯЗИ ИНТЕГРАЛЬНОЙ ОПТИЧЕСКОЙ ПЛОТНОСТИ ИЗОБРАЖЕНИЯ ТЕСТ - ОБЪЕКТА И РАЗРЕШАЮЩЕЙ СПОСОБНОСТИ В СИСТЕМАХ ЦИФРОВОЙ СТРУЙНОЙ И ЭЛЕКТРОФОТОГРАФИЧЕСКОЙ (ЭЛЕКТРОГРАФИЧЕСКОЙ) ПЕЧАТИ 481

Кайнарова Е.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна
ГЕНЕРАТИВНЫЙ ДИЗАЙН КАК ИНСТРУМЕНТ ДЕЯТЕЛЬНОСТИ ДИЗАЙНЕРА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И МЕДИА ИНДУСТРИИ 482

Канатенко М.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ЦИФРОВОЙ ПЕЧАТИ 483

Капуста Т.В., Яковлев П.О.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ИССЛЕДОВАНИЕ ПЕЧАТНО-ТЕХНИЧЕСКИЕХ СВОЙСТВ РАСХОДНЫХ МАТЕРИАЛОВ ОФСЕТНОЙ ПЕЧАТИ 483

Капуста Т.В., Абросимова Н.И., Абраменкова Ю.С.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ТЕХНОЛОГИИ ПЕЧАТИ ПО ТКАНЯМ 484

Коваленко А.Н.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ: ФОРМЫ И СВОЙСТВА..... 485

Костюк И.В., Козлова И.А., Алферов Н.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ЭФФЕКТИВНОГО ИСПОЛЬЗОВАНИЯ ИНТЕНСИВНЫХ КРАСОК В ОФСЕТНОЙ ИЛЛЮСТРАЦИОННОЙ ПЕЧАТИ 486

Костюк И.В., Малеваный К.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ ВОСПРОИЗВЕДЕНИЯ ИЗОБРАЖЕНИЙ СПОСОБОМ КАПЛЕСТРУЙНОЙ ПЕЧАТИ 487

Костюк И.В., Кюря В.П.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ТЕХНОЛОГИЯ УПРАВЛЕНИЯ ЦВЕТОМ ГЛУБОКОЙ ПЕЧАТИ НА ПОЛИМЕРНЫХ МАТЕРИАЛАХ С НЕСТАНДАРТНЫМИ ОПТИЧЕСКИМИ СВОЙСТВАМИ 488

Макарова Н.Е
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ОСОБЕННОСТИ РЕАЛИЗАЦИИ БАЗОВЫХ ФУНКЦИЙ ОБРАБОТКИ ТЕКСТА В СОВРЕМЕННЫХ ИЗДАТЕЛЬСКИХ СИСТЕМАХ И ЗАДАЧИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЕРСТКИ..... 489

Лысенко В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна
ТЕОРИЯ СОЗДАНИЯ. РАЗВИТИЕ 489

Павловская О.В., Дроздова Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна
ОСОБЕННОСТИ РЕДИЗАЙНА САЙТОВ 490

Приданов П.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет промышленных технологий и дизайна
РАЗРАБОТКА ПРОГРАММЫ ДЛЯ АВТОМАТИЧЕСКОЙ ПЛАНИРОВКИ ИНТЕРЬЕРА 490

Подкорытов С.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛИРОВАНИЕ ГЛАДКИХ САМОПОДОБНЫХ ПОВЕРХНОСТЕЙ 491

Тимофеева Е.А.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ВЕРСТКА ГАЗЕТЫ В ИНТЕРНЕТЕ 492

Трубникова А.М., Кузнецова Л.В.
Россия, Санкт-Петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологий и дизайна
ПРОБЛЕМЫ СНИЖЕНИЯ ЭФФЕКТИВНОСТИ ПОИСКА И ОБРАБОТКИ ИНФОРМАЦИИ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ 492

Чеботарева И.Б., Чеботарев Р.И., Муравьева А.В.
Украина, г. Харьков, Харьковский национальный университет радиоэлектроники
КОМПЛЕКСНАЯ ОЦЕНКА УРОВНЯ КАЧЕСТВА ФЛЕКСОПЕЧАТИ ТУБНОЙ УПАКОВКИ 493

Чеботарева И.Б.
Украина, г. Харьков, Харьковский национальный университет радиоэлектроники
ФОРМИРОВАНИЕ НЕЧЕТКИХ ОЦЕНОК ХАРАКТЕРИСТИК ЦИФРОВЫХ ОРИГИНАЛОВ 494

Шефер Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет промышленных технологий и дизайна, Высшая школа печати и медиатехнологий
КОМПЕНСАЦИЯ ВЛИЯНИЯ ДЕФЕКТОВ ФОРМЫ ПЕЧАТНЫХ ЦИЛИНДРОВ НА РАСТИСКИВАНИЕ ПУТЕМ ИЗМЕНЕНИЯ РАЗМЕРОВ РАСТРОВОЙ ТОЧКИ НА ДОПЕЧАТНОЙ СТАДИИ 495

Эрштейн Л. Б.
Россия, Санкт-петербург, Высшая школа печати и медиатехнологий Санкт-Петербургского университета промышленных технологий и дизайна
РАЗРАБОТКА ДИЗАЙНА ИНТЕГРИРОВАННОГО ИНТЕРФЕЙСА КАК СПОСОБ ОПТИМИЗАЦИИ РАБОТЫ ПОЛЬЗОВАТЕЛЯ С БАЗОЙ ДАННЫХ 496

ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ 497

Вавилов С.А., Лытаев М.С.
Россия, Санкт-Петербург, ЗАО «СПИИРАН-НТБВТ»
КАЛИБРОВКА И ВАЛИДАЦИЯ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ ЗОН ВИДИМОСТИ РЛС В ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ 497

Волгин П.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ МОНИТОРИНГА МОРСКОЙ ОБСТАНОВКИ 498

Ермолаев В.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ ИНТЕЛЕКТУАЛЬНЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ПРОЕКТИРОВАНИИ ГИДРОАКУСТИЧЕСКИХ СРЕДСТВ 499

Ивакин Я.А., Потапычев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ГЕОХРОНОЛОГИЧЕСКИЙ ТРЕКИНГ – СПЕЦИАЛИЗИРОВАННЫЙ ГИС-ИНСТРУМЕНТАРИЙ ИСТОРИЧЕСКОГО ИССЛЕДОВАНИЯ 499

Прокаев А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ ПОИСКОВЫМИ ДЕЙСТВИЯМИ В МОРЕ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ 500

Смирнова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
О МЕТОДЕ ПРОГНОЗИРОВАНИЯ И ВИЗУАЛИЗАЦИИ ЗОН ВИДИМОСТИ РЛС С ИСПОЛЬЗОВАНИЕМ ГИС-ИНСТРУМЕНТОВ 501

Цветков М.В., Васильев П.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПЛАНИРОВАНИЕ ЭКОЛОГИЧЕСКИХ ПОИСКОВО-СПАСАТЕЛЬНЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОЙ ГЕОГРАФИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МОНИТОРИНГА МОРСКОЙ ОБСТАНОВКИ 502

Штрапов В.В.
Республика Беларусь, г. Минск, Академия МВД Республики Беларусь
О НЕКОТОРЫХ АСПЕКТАХ ИСПОЛЬЗОВАНИЯ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 502

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ РИСКОМ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ 504

Алексеев В. В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН
ЛВ-АНАЛИЗ НАДЕЖНОСТИ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ МЕТАЛЛУРГИЧЕСКОГО КОМБИНАТА 504

Голоскоков К.П., Чиркова М.Ю.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРОБЛЕМА ПРОЕКТИРОВАНИЯ СИСТЕМЫ КОРПОРАТИВНОЙ БАЗЫ ЗНАНИЙ 504

Ежгуров В.Н., Доброрадова В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ПРЕДЛОЖЕНИЕ ПО РЕАЛИЗАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖАНИЯ И СОПРОВОЖДЕНИЯ ПРОЕКТОВ 506

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет
ПРЕДЛОЖЕНИЯ ПО ВНЕДРЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПЛАНИРОВАНИЯ ПРОИЗВОДСТВЕННЫХ ПРОГРАММ 506

Ежгуров В.Н., Егорова Н.В.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова,
Санкт-Петербургский государственный университет
ПРЕДЛОЖЕНИЯ ПО РАСШИРЕНИЮ В АВТОМАТИЗИРОВАННУЮ СИСТЕМУ УПРАВЛЕНИЯ ПРОЕКТАМИ ПОДСИСТЕМУ ОПТИМИЗАЦИИ ПРОЕКТОВ 507

Карасев В.В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН
ОЦЕНКА РИСКА ИНФРАСТРУКТУРЫ ЛОГИКО-ВЕРОЯТНОСТНЫМ МЕТОДОМ 508

Карасева Е.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
МЕТОДИКИ ОЦЕНКИ НАДЕЖНОСТИ БАНКА 509

Карасев В.В., Карасева Е.И.
Россия, Санкт-Петербург, Институт проблем машиноведения, Санкт-Петербургский государственный университет аэрокосмического приборостроения
УПРАВЛЕНИЕ БАНКОМ ПО КРИТЕРИЮ ИНТЕГРИРОВАННОГО РИСКА 510

Соложенцев Е. Д.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ ДИСЦИПЛИНЫ «УПРАВЛЕНИЕ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ» 511

Соложенцев Е. Д., Карасев В.В.
Россия, Санкт-Петербург, Институт проблем машиноведения РАН
БАЗЫ ДАННЫХ И УПРАВЛЕНИЕ РИСКОМ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТЬЮ СИСТЕМ 512

Крюкова Е.А., Козлова В.И. , Соложенцев Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
GlOBAL INNOVATIVE INDEX И КОМПЛЕКС ЛВ-МОДЕЛЕЙ ДЛЯ УПРАВЛЕНИЯ СИСТЕМАМИ ИННОВАЦИЙ..... 513

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ 514

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет
ПОДХОД К ОЦЕНКЕ ЗАЩИЩЁННСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК..... 514

Багрецов Г.И., Азаров А.А., Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербургский государственный университет
ПОДХОД К ПОСТРОЕНИЮ ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ..... 514

Березин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СИНТЕЗ ВТОРИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ: ПЕДЖИНАЦИЯ АЛГОРИТМА ГЕНЕРАЦИИ МНОЖЕСТВА МИНИМАЛЬНЫХ ГРАФОВ СМЕЖНОСТИ 515

Бирилло А.И.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ СОГЛАСОВАННОСТИ ОЦЕНОК ИСТИННОСТИ В ЛОКАЛЬНОМ АПРИОРНОМ И АПОСТЕРИОРНОМ ВЫВОДЕ В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ: ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ 515

Волков Н.В., Григорьев Д.А
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПРИМЕНЕНИЕ АОП-РЕФАКТОРИНГА В КРУПНЫХ CMS ПРОЕКТАХ ПРИ ПОМОЩИ ASPECT.NET 515

Григорьева А.В., Григорьев Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
БЕСШОВНАЯ ИНТЕГРАЦИЯ СРЕДСТВ ПРОВЕДЕНИЯ СОЦИАЛЬНЫХ ОПРОСОВ С ASP.NET MVC ВЕБ-ПРИЛОЖЕНИЯМИ НА ОСНОВЕ ASPECT.NET..... 516

Искрич Д.П, Григорьев Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПРИМЕНЕНИЕ ДЕРЕВЬЕВ РЕШЕНИЙ В ОБЛАСТИ БИРЖЕВОГО ТРЕЙДИНГА..... 517

Каспрук.Н.С.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»
АНАЛИЗ ИЗМЕРЕНИЙ ЦЕННОСТИ И СТРАТИФИКАЦИИ КЛИЕНТОВ ОТЕЛЕЙ НА ОСНОВЕ ОНЛАЙН-ДАННЫХ. СЛУЧАЙ САНКТ-ПЕТЕРБУРГА 518

Левенец Д.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ДЕКРЕМЕНТАЛЬНЫЙ СИНТЕЗ ВТОРИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ: СТАТИСТИЧЕСКАЯ ОЦЕНКА СЛОЖНОСТИ 518

Мальчевская Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
АРХИТЕКТУРА БИБЛИОТЕКИ ALGBNMODELLER: ПРЕДСТАВЛЕНИЕ АЛЬТЕРНАТИВНЫХ ФРАГМЕНТОВ ЗНАНИЙ..... 518

Мусабиров И.Л., Поздняков С.И., Бахитова А.А., Суворова А.В.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»,
Санкт-Петербургский институт информатики и автоматизации РАН
ПРОЕКТИРОВАНИЕ СОЦИАЛЬНОЙ СИСТЕМЫ ГЕЙМИФИКАЦИИ КУРСА
С ОНЛАЙН-КОМПОНЕНТОЙ 519

Нестеренко А. В., Мусабиров И. Л.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»
АНАЛИЗ СПЕЦИАЛИЗАЦИИ ИТ-РЫНКА НА ОСНОВЕ ДАННЫХ ОНЛАЙН-РЕКРУТИНГА 519

Поздняков С.И., Воскресенский В.М., Карепин В.В., Кузнецова А.Д., Федюнина А.А.,
Мусабиров И.Л.
Россия, Санкт-Петербург, НИУ «Высшая школа экономики»
ТЕМАТИЧЕСКИЙ КОНТЕКСТ В КАРТИРОВАНИИ ВЕБ-ПРИСУТСТВИЯ И НАУЧНО
ДЕЯТЕЛЬНОСТИ РОССИЙСКИХ ВУЗОВ. МЕТОДИКИ АНАЛИЗА 520

Столярова В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ НА ОСНОВЕ КОПУЛ ДЛЯ ПОСТРОЕНИЯ ОЦЕНКИ
ИНТЕНСИВНОСТИ УГРОЗООБРАЗУЮЩЕГО ПОВЕДЕНИЯ ИНДИВИДА ПО ДАННЫМ О
ОСЛЕДНИХ ЭПИЗОДАХ 521

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК ТЕСТОВЫХ ДАННЫХ В МОДЕЛИ ОЦЕНИВАНИЯ
ХАРАКТЕРИСТИК СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ 521

Торопова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
АНАЛИЗ СОГЛАСОВАННОСТИ ДАННЫХ В РАСШИРЕННОЙ МОДЕЛИ ОЦЕНКИ
СОЦИАЛЬНО-ЗГНАЧИМОГО ПОВЕДЕНИЯ 522

Харитонов Н.А., Мальчевская Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ЛОКАЛЬНЫЙ АПРИОРНЫЙ ВЫВОД В АБС: АВТОМАТИЗАЦИЯ АНАЛИЗА
ПРОПОЗИЦИОНАЛЬНОЙ ФОРМУЛЫ 522

Шиндарев Н.А., Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный университет
ПОСТРОЕНИЕ ВЕРОЯТНОСТНОЙ ГРАФИЧЕСКОЙ МОДЕЛИ ДЛЯ ОЦЕНКИ УСПЕШНОСТИ
СОЦИОИНЖЕНЕРНОЙ АТАКИ 522

**РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ,
ГРИД-ТЕХНОЛОГИИ 524**

Воробьев В.И., Петров М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МЕТОДЫ КОНВЕРГЕНЦИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И БОЛЬШИХ ДАННЫХ 524

Князева К.О., Воеводский К.С.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ: ПОНЯТИЕ И ВИДЫ 524

Копыльцов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
РАЗРАБОТКА ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ДЛЯ ОБРАБОТКИ СЛАБО ФОРМАЛИЗОВАННОЙ
ИНФОРМАЦИИ 525

Копыльцов А.В., Коршунов К.А., Лукьянов Г.Н., Серов И.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Фонд «АЙРЭС», Университет ИТМО
РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ
СО СТРУКТУРИРОВАННОЙ ПОВЕРХНОСТЬЮ 526

Кузнецов В.А.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
РАСПАРАЛЛЕЛИВАНИЕ ВЫЧИСЛЕНИЙ НА ГРАФИЧЕСКИХ ВИДЕОКАРТАХ 527

Ныркова А.П., Воеводский К.С., Князева К.О.
Россия, Санкт-Петербург, ГУМРФ им. адм. С.О. Макарова
ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ ПРИ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЁННОМ ХАРАКТЕРЕ ПРЕДПРИЯТИЯ 528

Уздяев М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ CUDA В ЗАДАЧАХ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ЛИЦ 529

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ» 531

Игнатьев М.Б., Попов В.П., Аксенов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМЫ СОЗДАНИЯ УМНЫХ АВТОМОБИЛЕЙ И ДОРОГ 531

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
АРТОНИКА И МОДЕЛИРОВАНИЕ ДРАМАТИЧЕСКИХ ПРОИЗВЕДЕНИЙ 531

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
МИР КАК МОДЕЛЬ ВНУТРИ МИРОВОГО СУПЕРКОМПЬЮТЕРА 532

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
СЕТЕЦЕНТРИЧЕСКИЕ СИСТЕМЫ УПРАВЛЕНИЯ 532

Попов В.П.
Россия,Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ДОСТОИНСТВА И НЕДОСТАТКИ УЖЕ ПОСТРОЕННЫХ УМНЫХ АВТОМОБИЛЕЙ. ОПЫТ ЭКСПЛУАТАЦИИ 533

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» 535

Абакумов А.А.
Россия, Санкт-Петербург, Университет ИТМО
РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДИК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ 535

Гатауллин Р.И.
Россия, Санкт-Петербург, Университет ИТМО
АНАЛИЗ ВОЗМОЖНОГО ПОВЕДЕНИЯ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУЛЬТИАГЕНТНОЙ СИСТЕМЕ ПРИ ИСПОЛЬЗОВАНИИ АЛГОРИТМОВ ФЛОКИРОВАНИЯ 535

Дикий Д.И., Рожкова Е.О., Артемьева В.Д., Савченко-Новопавловская С.Д.
Россия, Санкт-Петербург, Университет ИТМО
КЛИЕНТ-СЕРВЕРНОЕ ПРИЛОЖЕНИЕ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ПОЧЕРКУ 536

Зайцева Н.М.
Россия, Санкт-Петербург, Университет ИТМО
КОЛИЧЕСТВЕННАЯ ОЦЕНКА ПОТЕРЬ ОТ ПРАВОНАРУШЕНИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ .. 537

Золотарева Е.Н., Золотарева К.Н.
Россия, Санкт-Петербург, Университет ИТМО
КРИМИНАЛИСТИЧЕКАЯ ИДЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИОННЫЙ ПРИЗНАК В КИБЕРПРЕСТУПЛЕНИЯХ 537

Иоффе М.А., Нурдинов Р.А.
Россия, Санкт-Петербург, Университет ИТМО
ПОВЫШЕНИЕ ТОЧНОСТИ И ОБЪЕКТИВНОСТИ ОЦЕНКИ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ БЕЗОПАСНОСТИ 538

Канев А.Н., Настека А.В., Бессонова Е.Е.
Россия, Санкт-Петербург, Университет ИТМО
ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ СИСТЕМЫ «УМНЫЙ ДОМ» 539

Кривцова И.Е., Салахутдинова К.И.
Россия, Санкт-Петербург, Университе ИТМО
УСЛОВИЯ ПРИМЕНЕНИЯ КРИТЕРИЯ ПИРСОНА ДЛЯ ИДЕНТИФИКАЦИИ ИСПОЛНЯЕМЫХ ФАЙЛОВ..... 540

Коржук В.М., Демяшев А.Н.
Россия, Санкт-Петербург, Университет ИТМО
ПРОБЛЕМА УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ..... 540

Лейфер К.И.
Россия, Санкт-Петербург, Университет ИТМО
ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО БИОМЕТРИЧЕСКИМ ХАРАКТЕРИСТИКАМ ЖЕСТОВ НА СЕНСОРНОМ ЭКРАНЕ 541

Мурадов А.Р., Викснин И.И.
Россия, Санкт-Петербург, Университет ИТМО
ПРИМЕНЕНИЕ И АДАПТАЦИЯ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ АНАЛИЗА ПОВЕДЕНИЯ ТОЛПЫ В УСЛОВИЯХ ОГРАНИЧЕННЫХ ПРОСТРАНСТВ 542

Назыров М.В., Викснин И.И.
Россия, Санкт-Петербург, Университет ИТМО
ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ РАБОТЫ МОДЕЛИ ДВИЖЕНИЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ..... 542

Патрикеев Р.О., Щепин Н.Д.
Россия, Санкт-Петербург, Университет ИТМО
МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ БОЛЬШИХ СКОПЛЕНИЙ ЛЮДЕЙ В УСЛОВИЯХ РАЗЛИЧНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ 543

Ральникова Н.С.
Россия, Санкт-Петербург, Университет ИТМО
ДАКТИЛОСКОПИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ..... 544

Рожкова Е.О., Дикий Д.И.
Россия, Санкт-Петербург, Университет ИТМО
DLP-СИСТЕМА КАК СРЕДСТВО ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА 544

Спивак А.И., Спивак О.И., Шидакова Д.Н.
Россия, Санкт-Петербург, Университет ИТМО
УГРОЗЫ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ..... 545

Чалыкин И.Г.
Россия, Санкт-Петербург, Университет ИТМО
РАЗРАБОТКА СКАНЕРА УЯЗВИМОСТЕЙ СУБД ORACLE RDBMS..... 546

Цветков Л.В.
Россия, Санкт-Петербург, Университет ИТМО
ИСПОЛЬЗОВАНИЕ МОДЕЛИ ПРОГРАММНОГО КОДА ДЛЯ ОБНАРУЖЕНИЯ ПРОГРАММНЫХ ДЕФЕКТОВ 547

ОГЛАВЛЕНИЕ..... 548