ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2015)

IX САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2015 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2015

http://spoisu.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2015)

IX САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2015 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2015

http://spoisu.ru

УДК (002:681):338.98

И 74

Информационная безопасность регионов России (ИБРР-2015).
И 74 IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург,28-30октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. – 418 с.
ISBN 978-5-906782-83-0

Сборник охватывает широкий круг направлений: Государственная политика обеспечения информационной безопасности регионов России, Правовые аспекты информационной безопасности, Безопасность информационных технологий, Современные средства защиты информации, Информационная безопасность телекоммуникационных сетей, Информационно-экономическая безопасность, Информационная безопасность в критических инфраструктурах, Информационная безопасность в гидрометеорологии, Информационная безопасность в экологии, Информационная безопасность объектов морской техники и морской инфраструктуры, Информационно-психологическая безопасность, Информационная безопасность в социокомпьютинге, Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также включает материалы молодежной научной школы Безопасные информационные технологии.

Предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений Санкт-Петербурга и других регионов, специализирующихся в вопросах информационной безопасности 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*

Публикуется в авторской редакции

Подписано в печать 10.10.2015. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 25,8. Тираж500 экз. Заказ № 1045
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-906782-83-0

©Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2015 г.
© Авторы, 2015 г.

INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2015)

IX ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 28-30, 2015

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2015

http://spoisu.ru

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2015»

- 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 «ИБРР-2015»

- Российский фонд фундаментальных исследований
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- Санкт-Петербургский филиал «Ленинградское отделение Центрального научно-исследовательского института связи»
- ФГУП «ЦентрИнформ»
- Группа компаний «Омега»
- ЗАО «Ассоциация специалистов информационных систем»
- ЗАО «Институт инфотелекоммуникаций»
- ЗАО «Институт телекоммуникаций»
- ЗАО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- ОАО «Концерн «НПО «Аврора»
- ОАО «НПО «Импульс»
- ОАО «Центр компьютерных разработок»
- ООО «Геонавигатор»
- ООО «ИнТехСервис»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- 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
- Санкт-Петербургский государственный политехнический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
- Санкт-Петербургский государственный университет технологии 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
- Партнерство для развития информационного общества на Северо-Западе России
- Северо-западное отделение Российской академии образования
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии информатизации образования

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2015»

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
Балыбердин Александр Леонидович	Заместитель директора Административного департамента аппарата Правительства Российской Федерации
Велихов Евгений Павлович	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук
Ливанов Дмитрий Викторович	Министр образования и науки Российской Федерации
Никифоров Николай Анатольевич	Министр информационных технологий и связи Российской Федерации
Сергеев Алексей Иванович	Генеральный секретарь Совета Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств
Федоров Александр Вячеславович	Заместитель Председателя Следственного комитета Российской Федерации

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2015»

Советов Борис Яковлевич	Председатель Президиума, 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
Громов Иван Александрович	Председатель 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
Кучерявый Михаил Михайлович	Руководитель Управления ФСТЭК России по Северо-Западному федеральному округу
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»
Шульц Владимир Леопольдович	Заместитель президента Российской академии наук

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2015»

Председатель Организационного Комитета

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

Заместитель председателя Организационного Комитета

Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Алейник Ярослав Александрович	Руководитель Группы компаний «Омега»
Андронова Ольга Олеговна	Главный редактор газеты «Компьютер Информ»
Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Бакурадзе Дмитрий Викторович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Бачевский Сергей Викторович	Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Баскова Вячеслава Дмитриевича	Генеральный директор ООО «НеоБИТ»
Блажис Анатолий Константинович	Генеральный 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 ОАО «Научно-исследовательский институт программных средств»
Герус Евгений Валерьевич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»
Григорьев Владимир Александрович	Заведующий кафедрой «Беспроводные телекоммуникации» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, генеральный директор ООО «Лаборатория инфокоммуникационных сетей»
Гоголь Александр Александрович	Советник ректора, заведующий кафедрой «Телевидение и метрология» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Гуца Анатолий Григорьевич	Главный специалист СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Давыдов Евгений Борисович	Главный конструктор ФГУП «НИИ «Масштаб»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета технологии и дизайна
Долгирев Валерий Алексеевич	Помощник директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по защите информации

Жданов Сергей Николаевич	Заместитель генерального директора ЗАО «ВТБ-Девелопмент»
Жигадло Валентин Эдуардович	Заместитель генерального директора по развитию ЗАО «Институт телекоммуникаций»
Заборовский Владимир Сергеевич	Заведующий кафедрой «Телематика» Санкт-Петербургского государственного политехнического университета Петра Великого
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Директор Специализированного центра защиты информации, заведующий кафедрой «Информационная безопасность компьютерных систем» Санкт-Петербургского государственного политехнического университета Петра Великого
Зубков Юрий Сергеевич	Действительный государственный советник Санкт-Петербурга 3 класса
Идрисов Рустам Фидайович	Заместитель директора Центра исследований проблем безопасности Российской академии наук
Ипатов Олег Сергеевич	Заведующий кафедрой «Программно-аппаратные комплексы реального времени», Санкт-Петербургского государственного политехнического университета Петра Великого
Искандеров Юрий Марсович	Заместитель директора ЗАО «Институт проблем транспорта им. Н.С. Соломенко Российской академии наук»
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга
Кирсанов Игорь Петрович	Генеральный директор ЗАО «Выставочное Объединение «РЕСТЭК»
Корниенко Анатолий Адамович	Заведующий кафедрой «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения
Кузичкин Александр Васильевич	Заместитель директора ФГУП «Научно-исследовательский институт 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)
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
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности
Николаев Алексей Юрьевич	Генеральный директор ЗАО «Эврика»
Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Ныркov Анатолий Павлович	Заведующий кафедрой «Комплексное обеспечение информационной безопасности» 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
Перепелица Сергей Николаевич	Генеральный директор ООО «ИнТехСервис»
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
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 ЗАО «Ассоциация специалистов информационных систем»
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 ОАО «НПО «Импульс»
Уткин Виктор Викторович	Директор Центра электронных образовательных технологий и ресурсов Международного банковского института
Федоров Андрей Евгеньевич	Директор института – заместитель генерального директора ОАО «Концерн «НПО «Аврора»
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Цыулев Сергей Валентинович	Главный специалист Отдела информационно-компьютерной безопасности Комитета по информатизации и связи
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Российской академии наук
Чугунов Андрей Владимирович	Заведующий кафедрой «Управление государственными информационными системами», директор Центра технологий электронного правительства Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Шерстюк Юрий Михайлович	Генеральный директор ЗАО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор ОАО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2015»

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций»
Молдовян Александр Андреевич	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук по информационной безопасности

Члены Программного Комитета

Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор Санкт-Петербургского государственного морского технического университета, доктор технических наук, профессор
Азаров Артур Александрович	Старший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, кандидат технических наук
Балыкбаева Улбосын Айтуаровна	Инженер ЗАО «Ассоциация специалистов информационных систем»
Бариков Леонид Николаевич	Доцент Санкт-Петербургского государственного университета аэрокосмического приборостроения, кандидат технических наук, доцент
Берекет Виктор Максимович	Генерал-майор полиции, заместитель начальника Санкт-Петербургского университета МВД России по научной работе, кандидат юридических наук, доцент
Бессонова Екатерина Евгеньевна	Ассистент кафедры «Безопасные информационные технологии» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Бузников Анатолий Алексеевич	Заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), заслуженный деятель науки Российской Федерации, доктор технических наук, профессор
Буйневич Михаил Викторович	Профессор Санкт-Петербургского государственного экономического университета, доктор технических наук, профессор
Вассоевич Андрей Леонидович	Профессор кафедры «Политическая психология» Санкт-Петербургского государственного университета, доктор философских наук, профессор
Виноградов Александр Андреевич	Заместитель главного конструктора ОАО «НПО «Импульс», кандидат технических наук
Владимирова Оксана Михайловна	Инженер кафедры «Океанология», председатель Студенческого научного общества Российского государственного гидрометеорологического университета
Волков Виктор Иванович	Ведущий научный сотрудник Военного учебно-научного центра Военно-морского флота «Военно-морская академия», заслуженный деятель науки Российской Федерации, доктор технических наук, профессор
Воробьев Владимир Иванович	Главный научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор технических наук, профессор
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, кандидат технических наук, дважды лауреат Премии Правительства Российской Федерации в области образования
Горохов Владимир Леонидович	Профессор, Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, доктор технических наук, профессор

Дмитриева Марина Владимировна	Сотрудник аппарата Санкт-Петербургского Регионального отделения Союза машиностроителей России
Домбровская Лариса Александровна	Профессор кафедры «Математика и информатика» Санкт-Петербургского университета МВД России, кандидат педагогических наук, доцент
Зикратов Игорь Алексеевич	Заведующий кафедрой «Безопасные информационные технологии» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, доктор технических наук, профессор
Игнатьев Михаил Борисович	Заслуженный профессор Санкт-Петербургского государственного университета аэрокосмического приборостроения, доктор технических наук, профессор, Distinguished Scientist of the Association of Computing Machinery, лауреат Государственной премии СССР, лауреат премии Президента Российской Федерации в области образования
Игумнов Владимир Вячеславович	Первый заместитель генерального директора, главный конструктор ОАО «НПО «Импульс», кандидат технических наук
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, лауреат премии Правительства Российской Федерации в области образования, кандидат технических наук, доцент
Кефели Игорь Федорович	Заведующий кафедрой «Глобалистика и геополитика» Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова, заслуженный работник высшей школы Российской Федерации, доктор философских наук, профессор
Кий Андрей Вячеславович	Старший преподаватель Военной академии связи им. С.М. Буденного, кандидат технических наук
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, доктор технических наук, профессор
Коноплёв Георгий Асадович	Доцент Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), кандидат технических наук, доцент
Корниенко Анатолий Адамович	Заведующий кафедрой «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения, доктор технических наук, профессор
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор технических наук, профессор
Крук Евгений Аврамович	Директор Института информационных систем и защиты информации Санкт-Петербургского государственного университета аэрокосмического приборостроения, доктор технических наук, профессор, лауреат премии Правительства Санкт-Петербурга, заслуженный деятель науки Российской Федерации
Лебедев Илья Сергеевич	Доцент кафедры «Безопасные информационные технологии» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, доктор технических наук, доцент

Левкин Игорь Михайлович	Профессор Санкт-Петербургского государственного экономического университета, доктор военных наук, профессор
Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, кандидат экономических наук
Митько Арсений Валерьевич	Доцент кафедры «Морские информационные системы» Российского государственного гидрометеорологического университета, председатель Совета молодых учёных Севера Арктической общественной академии наук, кандидат технических наук, доцент
Митько Валерий Брониславович	Профессор кафедры «Морские информационные системы» Российского государственного гидрометеорологического университета, председатель Санкт-Петербургского отделения секции геополитики и безопасности Российской академии естественных наук, президент Арктической общественной академии наук, доктор технических наук, профессор
Молдовян Николай Андреевич	Заведующий лабораторией криптологии Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор технических наук, профессор, заслуженный изобретатель Российской Федерации
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Невзоров Станислав Васильевич	Директор «Центра импортозамещения»
Новикова Евгения Сергеевна	Доцент кафедры «Автоматизированные системы обработки информации и управления» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), кандидат технических наук, доцент
Ныркov Анатолий Павлович	Заведующий кафедрой «Комплексное обеспечение информационной безопасности» Государственного университета морского и речного флота имени адмирала С.О. Макарова, доктор технических наук, профессор
Овчинников Андрей Анатольевич	Доцент кафедры «Безопасность информационных систем» Санкт-Петербургского государственного университета аэрокосмического приборостроения, кандидат технических наук, доцент
Паращук Игорь Борисович	Профессор Военной академии связи им. С.М. Буденного, доктор технических наук, профессор
Плебанек Ольга Васильевна	Доцент кафедры «Глобалистика и геополитика» Балтийского государственного технического университета «ВОЕНМЕХ» им. Д.Ф. Устинова, кандидат философских наук, доцент
Примакин Алексей Иванович	Полковник полиции, начальник кафедры «Специальные информационные технологии» Санкт-Петербургского университета МВД России, доктор технических наук, профессор
Путилин Алексей Николаевич	Заместитель главного конструктора ОАО «НПО «Импульс», доктор технических наук, профессор
Пылаев Александр Юрьевич	Главный редактор журнала «Экспертный союз»

Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор технических наук, профессор
Самойленко Елена Александровна	Инженер ЗАО «Ассоциация специалистов информационных систем»
Свешникова Наталья Олеговна	Доцент кафедры «Политическая Психология» факультета психологии Санкт-Петербургского государственного университета, кандидат психологических наук, доцент
Согонов Сергей Александрович	Заведующий кафедрой «Судовая автоматика и измерения» Санкт-Петербургского государственного морского технического университета, кандидат технических наук, доцент
Соколов Сергей Сергеевич	Доцент кафедры «Комплексное обеспечение информационной безопасности» Государственного университета морского и речного флота имени адмирала С.О. Макарова, кандидат технических наук, доцент
Солодянников Александр Владимирович	Генеральный директор ЗАО «Ассоциация специалистов информационных систем», кандидат экономических наук, доцент
Татарникова Татьяна Михайловна	Профессор Санкт-Петербургского государственного экономического университета, доктор технических наук, доцент
Трофимов Валерий Владимирович	Заведующий кафедрой «Информатика» Санкт-Петербургского государственного экономического университета, заслуженный деятель науки Российской Федерации, доктор технических наук, профессор
Тулупьев Александр Львович	Заведующий лабораторией теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, доктор физико-математических наук, доцент
Тюрин Иван Сергеевич	Системный аналитик НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Устинов Игорь Анатольевич	Генеральный директор ОАО «Научно-производственное объединение «Импульс», кандидат технических наук
Ушакова Наталья Петровна	Заведующая лабораторией ОАО «Концерн «НПО «Аврора», кандидат технических наук, доцент
Цехановский Владислав Владимирович	Заведующий кафедрой «Автоматизированные системы обработки информации и управления», профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), лауреат премии Правительства Санкт-Петербурга, кандидат технических наук, доцент
Цыулёв Сергей Валентинович	Главный специалист Отдела информационно-компьютерной безопасности Комитета по информатизации и связи
Шакин Дмитрий Николаевич	Заместитель руководителя Управления ФСТЭК России по Северо-Западному федеральному округу, кандидат военных наук, доцент
Шишкин Владимир Михайлович	Старший научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, кандидат технических наук, доцент

Шкирятов Олег Тимофеевич	Первый заместитель генерального директора по научной работе ОАО «Научно-производственное объединение «Импульс», доктор военных наук, профессор
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры «Математика и информатика» Санкт-Петербургского университета МВД России, кандидат психологических наук

Ученый секретарь Конференции

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

Координатор Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга

Информационное обеспечение Конференции

«Компьютер Информ»	Газета о передовых инфокоммуникационных технологиях, продуктах, решениях для руководителей предприятий и организаций, отделов АСУ, ведущих специалистов и служб ИКТ, http://www.ci.ru
«Экспертный союз»	Информационно-аналитический журнал Санкт-Петербургского регионального отделения Общероссийской общественной организации «Союз машиностроителей России»,http://www.unionexpert.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

Юсупов Р.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ ОТЕЧЕСТВЕННОЙ НАУКИ И ОБРАЗОВАНИЯ НА СОВРЕМЕННОМ ЭТАПЕ

Наука и образование рассматриваются как единый организм – научно-образовательный комплекс, характеризующийся различными моделями их взаимодействия.

В докладе обсуждаются основные факторы, влияющие на развитие науки в РФ после распада СССР: попытка создать новую академию наук России, проблемы финансирования и кадрового обеспечения науки, рост экспорта «научного сырья», «наступление» технонауки, реформирование государственных академий и т.д. Показывается, как все это влияет на изменение структуры научной сферы в целом и РАН в частности.

Отмечаются основные тренды в структуризации высшей школы: утверждение особого статуса МГУ и СПбГУ, создание федеральных университетов, национальных исследовательских университетов и программы «5х100х2020».

Болгов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПОЛИТИКА РОССИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ

В докладе представлены подходы к политике кибербезопасности внутри России, а также показано, как внутренняя политика кибербезопасности России влияет на внешнюю, т.е. на международные инициативы России и на ее участие в соответствующих международных структурах. В исследовании представлены два основных подхода к вопросам кибербезопасности в российском политическом и экспертном сообществе, существующие с 1990-х годов: либерально-идеалистический и обскурантистский. Проанализированы основные документы, регулирующие вопросы кибербезопасности в России: Доктрина информационной безопасности (2000), Государственная программа «Информационное общество» (2011), Основы государственной информационной политики РФ в области международной информационной безопасности на период до 2020 г. (2013), Военная доктрина (в ред. 2014 г.), Государственная программа вооружения до 2020 г., федеральные законы, касающиеся отдельных сторон кибербезопасности, а также концепция Стратегии кибербезопасности (2013).Также рассмотрены основные акторы в данной сфере и их полномочия: государственные силовые ведомства (ФСБ и другие спецслужбы, Министерство обороны), бизнес, сообщества экспертов. Сделан вывод о том, что ключевую роль здесь играет сегодня ФСБ, особенно за счет монопольного установления стандартов кибербезопасности, поскольку все ведомства обязаны пользоваться средствами защиты информации, сертифицированными ФСБ.

У России пока что отсутствует отдельная киберстратегия в виде официального документа. В российской армии модернизация в данной сфере движется медленными темпами. Киберкомандование (его планировалось сформировать по американскому образцу) до сих пор не создано, хотя об этом много говорили на правительственном уровне. Войска информационных операций были созданы в 2014 г., однако их формирование шло форсировано и не всегда обдуманно (изначально планировалось завершить их формирование к 2017 г.)Достаточно проблемной остается сфера разработки и производства электронной компонентной базы для российского ВПК. Сегодня используется более 60% элементной базы иностранного производства.

Поскольку Россия последовательно делает акцент на нормативно-правовом регулировании вопросов кибербезопасности на внутринациональном уровне(особенно в последние годы, если посмотреть на количество принятых документов), этого же подхода она придерживается и на международном уровне: вопросы кибербезопасности нужно регулировать, причем как можно скорее и как можно более детально. Этого подхода Россия придерживалась на протяжении 15 лет, предлагая свои проекты в рамках ООН (в частности, предложение о создании специального международного суда по преступлениям в информационной сфере). Россию поддерживали Китай, Индия и Бразилия. Однако это наталкивалось на противоположную позицию США, ЕС и Японии, считающих, что вопросы

кибербезопасности не нужно излишне «перерегулировать» в ущерб свободам граждан и бизнеса. Некоторое сближение позиций по данным вопросам наметилось на конференции по безопасности в Мюнхене в феврале 2011 г., где большинство политиков и экспертов высказалось за необходимость международно-правового регулирования киберпространства. Несмотря на то, что был подготовлен совместный российско-американский доклад, конкретных решений обязательного характера принято не было.

Неудачи России в проведении своих инициатив по кибербезопасности через ООН (с 1998 г.) подстегнули актуализацию Россией этих вопросов в повестке дня Шанхайской организации сотрудничества (ШОС). Китай и Казахстан с 2011 г. также рассматривают данную организацию как инструмент для контроля киберпространства. Во время председательства России в 2014 г. в Шанхайской организации сотрудничества кибербезопасность была одним из приоритетов повестки дня, определенных Россией в этой организации.

Еще одним инструментом продвижения интересов России в сфере кибербезопасности становится формат БРИКС. В рамках этой структуры борьба с киберугрозами названа одном из четырех сфер перспективного сотрудничества. Обсуждаются идеи создания Центра киберугроз БРИКС, а также «горячей линии» для информирования и предупреждения о киберинцидентах наподобии той, которая уже существует между Россией и США.

Перед Олимпийскими играми в Сочи в 2014 г. сенатор Р. Гаттаров предлагал создать штаб по обеспечению информационной безопасности олимпийских объектов, но штаб так и не был создан.

Таким образом, главной правовой проблемой можно назвать отсутствие единого и целостного международного законодательства в сфере регулирования киберпространства. Сегодня действуют только отдельные нормы международного права или национальных законодательств. Проблемой можно также назвать противоречивость отдельных положений внутри источников международного права (в частности, в Международном телекоммуникационном соглашении 1973 г.), которые могут использоваться акторами в своих интересах.

Бондуровский В.В.,Вус М.А.
Россия, Санкт-Петербург, Секретариат Совета Парламентской Ассамблеи Организации Договора о коллективной безопасности, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ЗАКОНОДАТЕЛЬСТВО ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ ОДКБ

В УставеОрганизации Договора о коллективной безопасности (ОДКБ) обеспечение информационной безопасности закреплено как важное направление сотрудничества государств, её членов.Развитие системы обеспечения международной и коллективной безопасности зависит сегодня от единого понимания и трактовок подходов к формированиюсистемы информационной безопасности. Под системой информационной безопасности в политических и правовых документах ОДКБ понимаетсякомплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и социального характера, нацеленных на обеспечение информационной безопасности государств – членов.

Реалии международных отношений актуализируют задачи развития сотрудничества в рамкахПарламентской Ассамблеи ОДКБ (ПА ОДКБ).Укреплениеправовой составляющей информационной безопасности с необходимостью требуетпарламентского измерения и реализации потенциала парламентской дипломатии.Правотворческая деятельность ПА ОДКБ осуществляется на основе Программы по сближению и гармонизации национального законодательства государств – членов ОДКБ.Над проектами правовых актов и рекомендаций работают парламентарии и специалисты-эксперты. В целях научно-методического обеспечения разработки проектов документов, предусмотренных Программой, на регулярной основе выполняются сравнительно-правовые анализы законодательства государств – членов ОДКБ.

Вопросы сближения и гармонизации законодательства государств – членов ОДКБ в области обеспечения информационной безопасности обсуждались на международной научно-практической конференции «Законодательство государств – членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации» (2013), в рамках Национального и Евразийских форумов по информационной безопасности (2012-2015).

Сегодня необходима всесторонняя углубленная научная проработка принципиальных целей, задачи направлений развития сотрудничества государств по противодействию современным угрозам в информационной сфере. Это, в свою очередь, требует определенности и однозначности понятийного аппарата модельного и национального законодательства, развития системы терминов и понятий, закрепление их определений в нормативных актах, а также правового толкование понятийного аппарата в общественном обращении и повседневной практике. Назрела необходимость системного совершенствования информационного законодательства, отражающего новые реалии, практику и общественные интересы в области информационной безопасности.

Для эффективного взаимодействия и сотрудничества органам власти и управления, субъектам хозяйственной деятельности, физическим и юридическим лицам различных государств необходимы сведения, основанные на едином понимании предметов и явлений информационного пространства регулируемого законодательными положениями. В целях актуализации существующего понятийного аппарата СПИИРАН подготовил и выпустил в свет «Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ» (СПб, 2014), аккумулировавший понятийный аппарат из национального и законодательства и важнейших международно-правовых документов в рассматриваемой сфере.

Врамках Программы ПА ОДКБ по сближению и гармонизации законодательства был выполнен сравнительный анализ национального законодательства государств – членов ОДКБ в сфере информационной безопасности (2013-2014). На основе результатов проведённого интернациональным коллективом российских и белорусских учёных анализа разработаны Рекомендации по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности (2014), принятыеПА ОДКБ.

Алейник Я.А.
Россия, Санкт-Петербург, Группа компаний «Омега»

ИМПОРТОЗАМЕЩЕНИЕ. ВОЗМОЖНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ПЛАТФОРМЕ 1С:ПРЕДПРИЯТИЕ ПРИ ПОДКЛЮЧЕНИИ К ГИС - ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТАМОЖЕННЫХ ОРГАНОВ

В докладе рассматриваются информационные процессы в управлении, их состав и особенности функционирования в комплексных системах управления в таможенном деле. Особое внимание уделяется техническому, технологическому, информационному и программному видам обеспечения с учетом потребностей таможни в условиях работы в автоматизированных информационных системах на основе «1С:Предприятие 8».

В докладе раскрывается сущность информационной системы «1С:Предприятие»8 которая представляет собой универсальную систему для автоматизации учета и может быть адаптирована к любым особенностям на конкретном предприятии при помощи модуля «1С:Конфигуратор», позволяющего настраивать все основные элементы программной среды, генерировать и редактировать документы с любой структурой, изменять их экранные и печатные формы, формировать журналы для работы с документами с возможностью их произвольного распределения по журналам.

Важное место в автоматизации таможенного дела занимает консультационная, технологическая и методическая поддержка пользователей "1С:Бухгалтерии 8". В докладе выявляются области применения платформы «1С:Предприятие 8» в организациях таможни, где информационный поток превышает 20 тыс. документов в сутки. Применяется более 300 видов электронных документов и сообщений в квартал. Реализована ежеквартальная версионность бизнес-процессов, а области применения платформы «1С:Предприятие 8» в таможенных организациях организации эффективно расширены. В докладе раскрываются новые горизонты применения платформы «1С:Предприятие 8» в организации.

Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОСОБЕННОСТИ РАЗРАБОТКИ БЕЗОПАСНЫХ ПРИЛОЖЕНИЙ В ОБЛАКЕ ДЛЯ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Вопросы обеспечения информационной безопасности облачных приложений лежат в нескольких плоскостях – технической, юридической и организационной.

Разработке безопасных приложений посвящено много технических материалов. Написана масса статей и обзоров как, что и где настроить. Однако проблема в этой области остается из-за наличия человеческого фактора и отсутствия квалифицированного персонала, знакомого с облачной инфраструктурой конкретного поставщика. Статистика рынка труда служит тому доказательством.

Нормативная база. Юридический аспект: облачные технологии являются сравнительно новыми технологиями. Обеспеченность стандартами в области информационной безопасности (ИБ) облачных решений в настоящий момент не достаточна. Количество стандартов можно пересчитать по пальцам. Российские стандарты отсутствуют. Узкоспециализированные стандарты (например, международный стандарт защиты персональных данных в облаке ISO/IEC 27018: 2014) начали только появляться, начинает нарабатываться практика их использования.

Приложение в рамках реализации принципа “единого окна”, специализированный портал гос. услуг или аналогичное программно – аппаратное решение (в котором могли бы использоваться облачные технологии в той или иной мере) до недавнего времени с точки зрения разработки с учетом требований ИБ требовало соблюдения ряда требований законодательства.

В последнее время количество внедрений с использованием облачных технологий различных вендоров для органов государственной власти, постоянно растет. Следует отметить, что в основе подобных решений используются в той или иной мере облачные среды зарубежных фирм - разработчиков или решения отечественных ИТ - компаний, базирующиеся на использовании зарубежных облачных продуктов.

Организационный аспект. В связи со сложившейся обстановкой (введением санкцийпротив РФ, др. факторов) законодательство предписывает хранить данные в центрах обработки данных на территории страны.А в соответствии с меняется порядок государственных закупок в области информационных продуктов и подписки на ИТ - сервисы зарубежного производства (что делает использование облачных сред зарубежных разработчиков затруднительным).

Все эти “особенности” в текущих реалиях могут негативно сказаться на возможностях разработки облачных приложений для нужд государственной власти, в особенности тех, где требуется решение вопросов, связанных с ИБ данных, обеспечения безопасного доступа. Однако обзор открытых источников показывает, что ИТ – компаний есть ряд ”рецептов” и “наработок”, как продолжить создавать безопасные облачные приложения для различных гос. структур.

Брысова В.А., Шубинский М.И.
Россия, Санкт-Петербург, Администрация Петроградского района, ИМЦ Петроградского района

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ШКОЛЫ НА ПРИМЕРЕ ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

Один из самых важных вопросов стоящих сейчас перед любым государственным учреждением с точки зрения информационных технологий – это вопрос информационной безопасности. Однако особенно остро эти вопросы стоят перед учреждениями среднего образования.

Школа должна выполнять все требования федерального законодательства по защите информации и безопасности персональных данных. В Петербургских школах, в настоящий момент в среднем 50-80 компьютеров, объединенных в локальную сеть. В типовом образовательном учреждении (в дальнейшем ОУ) имеются 2-3 сервера, различного назначения и ведется минимум 3-4 информационные системы, содержащие персональные данные и сотрудники школ (учителя, инженеры) не имеют должной квалификации в вопросах защиты информации.

Подробнее разберем задачи, решающиеся на тех или иных компьютерах.

Компьютеры в компьютерных классах предназначены для обучения учащихся на уроках «основы ИКТ» или интегрированных уроках по иным предметам. Для ведения обучения на данных компьютерах требуется выход в сеть Интернет и установка, требуемых педагогических программных средств (ППС). Занятия ведутся под контролем учителя. Компьютеры в медиатеке предназначены для самостоятельной работы педагогов и учащихся. Компьютеры должны быть подключены к сети Интернет и к школьному файловому серверу. Компьютеры в учебных кабинетах предназначены для подготовки учителей к урокам, ведению электронного классного журнала и к работе на уроке с мультимедийным проектором и интерактивной доской. Компьютеры в учительской предназначены для подготовки учителей к урокам, ведению электронного классного журнала. Компьютеры в бухгалтерии работают с бухгалтерской программой (например, системой 1С-бухгалтерия) и АИС «Госзаказ» (АИС ГЗ).

Компьютер директора должен быть подключен к Интернету и не нем должен быть настроен официальный электронный адрес учреждения. На компьютере должно стоять специальное ПО для работы с ЭЦП для АИС ГЗ и АИС «Электронный торги», на нем должен быть доступ к файлам с управленческими документами (приказами, письмами, тарификацией и т.п.) и ко всем основным модулям автоматизированной системы управления образовательным учреждением АИС «Параграф» (Кадры, движение учащихся, классный журнал, учебный план и т.п.). Компьютер должен быть связан локальной сетью с остальными управленческими компьютерами.

Компьютеры секретаря и заместителей директора тоже должны быть связаны в единую локальную сеть, иметь доступ в Интернет. На них на всех должен быть настроен вход в АИС «Параграф» с соответствующими правами.

К файловому серверу должен быть доступ у всех компьютеров, правда с возможностью разграничить доступ логически к тем или иным разделам, а на сервере баз данных стоит серверная часть АИС «Параграф». Компьютеры инженерной службы имеют администраторские права с полным доступом ко всем приложениям.

Все вышеперечисленное говорит о том, что в упрощенном случае локальная сеть учреждения должна быть разбита минимум на 3 сегмента (или домена).

Машины, на которых работают учащиеся (компьютерные классы и медиатека). С данных машин должен быть невозможен доступ к базам данных, учительским и административным компьютерам. Учительские компьютеры (в учебных кабинетах и учительской). Из данного сегмента сети должен быть невозможен доступ к управленческим компьютерам, но требуется выход к АИС «Параграф».

При этом необходимо помнить, что учителям необходимо с одного и того же компьютера и выходить в Интернет и работать в АИС «Параграф». Однако, такая одновременная работа не устраивает специалистов по информационной безопасности. В качестве выхода из данной ситуации в Петроградском районе, с помощью КИС и ИАЦ, было решено поставить в школы для учителей не обычные компьютеры, а программно-аппаратный комплекс защиты информации ALTELL FORT DT5. Эти комплексы на одном рабочем месте включают в себя предустановленное программное обеспечение ALTELL TRUST и программное обеспечение СКЗИ КриптоПро CSP версии 3.9.

На данный момент планируется, что работа учителей на программно-аппаратном комплексе защиты информации ALTELL позволит развивать в школе информационную безопасность.

Волков Ю.Д.
Россия, Саранск, Мордовский государственный университет им. Н.П. Огарева

ИНТЕЛЛЕКТУАЛИЗАЦИЯ ЭКСПЕРИМЕНТА В АВТОНОМНЫХ ЭНЕРГОСИСТЕМАХ: ПРОБЛЕМНО-ОРИЕНТИРОВАННЫЙ ПОДХОД

Концепция интеллектуализации эксперимента рассматривается на примере автономных энергосистем (АвЭС), которые относятся к сложным человеко-машинным системам, основной функцией которых является бесперебойное и качественное снабжение энергией потребителей.

В зависимости от количества и качества исходной информации об объекте исследований рассматриваются различные задачи и модели эксперимента с учетом неопределенности. Неопределенность эксперимента, возникающая при поиске решения задачи, связана с неточностью измеряемых параметров, приборов, невозможностью проведения эксперимента в аварийных режимах, необходимостью принимать решения с использованием экспертных знаний, случайным характером нагрузки АвЭС, отказом оборудования, влиянием помех и многими другими факторами.

В условиях неопределенности выбор моделей, методов и средств интеллектуализации эксперимента определяется уровнем знаний о решаемой проблеме. В нашем понимании под проблемой будем понимать сложный вопрос, задачу (осознанную и сформулированную), требующую разрешения, моделирования, экспериментального исследования группы взаимоисключающих гипотез, выдвигаемых относительно объекта исследований.

Ориентация на проблему, на знания о решаемой задаче является основой такого научного направления, как проблемно-ориентированные исследования и выступает свидетельством большой степени неопределенности в познании и деятельности. Такие философские подходы, используемые в качестве научного познания, лучше всего выражают эвристический потенциал научных исследований через демонстрацию своих возможностей, пределов.

Проблемно- ориентированный подход предполагает ориентацию на специализированные методы решения задач, принадлежащих некоторому четко выделяемому классу. Выделение класса производится либо фиксацией математических объектов, лежащих в основе решаемых задач, либо фиксацией области применения компьютеров (напр. класс задач оперативного управления). Основываясь на проблемно-ориентированном подходе и уровне знаний о решаемой проблеме можно выделить три группы, относящиеся к классу задач активного эксперимента:

1. задачи при отсутствии каких-либо оценок относительно вероятностей гипотез;
2. вероятностные задачи, при известном исходном распределении вероятностей гипотез;
3. нечеткие задачи, то есть при нечеткой оценке вероятностей гипотез.

Задача 1 решается в рамках дискретной модели эксперимента в пространстве состояний. На начальном этапе эксперимента отсутствуют знания об исходном распределении вероятностей гипотез (задача 1), поэтому положим равными значения вероятностей. По мере проведения эксперимента будем осуществлять байесовский пересчет вероятностей.

Однако, при решении сложных экспериментальных задач следует учитывать случайный характером проведения измерений, воздействием внешней среды и других факторов. Эту неопределенность отразим в рамках вероятностной модели эксперимента. Возможно, что нам априори известны вероятности гипотез из ранее набранной статистики. Знание вероятностей позволяет произвести целенаправленный эксперимент и уменьшить его стоимость.

Поиск в вероятностном пространстве состояний S предпочтителен при решении специфичных задач с пространством S небольшой размерности. Модель не учитывает наличие знаний о предметной области и неопределенность, возникающую уже на стадии выдвижения гипотез. Для реализации этой модели необходимо знание исходного распределения вероятностей.

При отсутствии точечной оценки вероятностей гипотез на ранних стадиях эксперимента применим лингво-численную оценку, например: вероятность гипотезы составляет «около или близко к 0,3». Данная оценка заменяется нечеткими FN-числами. Функции принадлежности данных чисел приводятся в упрощенном модифицированном LR-формате, который выбирается из условия минимума отклонения от нормального закона. Для модели обработки измерительной информации, полученной на ранних стадиях эксперимента, предлагается арифметика нечетких FN-чисел.

Рассматриваются различные критерии оптимизации эксперимента (энергозатраты, достоверность, энтропия).

Проблемно-ориентированный подход, в рамках которого формируется контекст когнитивной ситуации, создает наиболее адекватные эвристические условия для исследовательского процесса в АвЭС.

Горелик С.Л., Лещинский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ЗАЩИТА ОТЧЕТНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННЫХ ИСКАЖЕНИЙ В СИСТЕМАХ УЧЕТА ПАССАЖИРСКОГО ТРАНСПОРТА

Разработка современной электронной системы оплаты проезда на пассажирском транспорте должна быть интегрирована с АСУ наземного пассажирского транспорта и включать систему защиты от использования в целях искажения отчетности, уклонения от налогообложения и незаконного получения субсидий.

Система защиты должна быть автономной и использовать решения, основанные на сравнительной оценке функций коррелированных параметров, получаемых по различным выборкам исходных данных в процессе мониторинга систем оплаты и управления. Такая система должна обеспечивать следующие функции:

– выявление искажений данных отчетности в результате технических проблем или умысла пользователей;

– самообучение на основе, выявленных и исправленных с участием экспертов, злоупотреблений;

– обеспечение специальных мер по маскировке алгоритмов, используемых в системе защиты, для предотвращения противодействия со стороны недобросовестных пользователей

При разработке систем оплаты и АСУ пассажирского транспорта должны быть обеспечены организационно-технические мероприятия (разделение разработчиков на группы, ограничение доступа к документам и материалам, содержащим сведения, которые могут быть использованы недобросовестными пользователями систем или злоумышленниками). Должны учитываться также и возможные угрозы по дезорганизации транспортной системы, которые могут привести к значительным финансовым потерям и представлять угрозу для пассажиров и других участников движения.

Существенное улучшение существующих систем оплаты основано на использовании технологии «связки ключей», в которой базовым идентификатором является номер мобильного коммуникатора пользователя, с использованием существующих идентификаторов, которые используются для оплаты и доступа в отдельных приложениях, в соответствии с установленным там и используемым периферийным оборудованием, в качестве дополнительных тем самым, обеспечивая совместимость с действующими системами различных типов для снижения затрат на стартовом периоде.

Данные о текущем счете клиента хранятся на сервере системы, но, при необходимости, имеется опция, позволяющая записывать на дополнительные носители (карты) сведения о платежном кредите и льготах пользователя в ограниченном объеме и синхронизировать эти данные с хранящимися на карте в режиме оффлайн, но со специальными мерами, предусматривающими невозможность злоупотребления в период между обменом данными в моменты синхронизации.

При использовании указанного варианта построения системы не требуется полная переработка существующих систем, а только уточнение и согласование некоторых алгоритмов и параметров. При таком подходе та часть работ, которая связана с созданием связки ключей и синхронизацией данных и некоторые варианты схемы оплаты в местах оказания услуг, а также подключение к системе пополнения текущих учет через банковские карты, платежные системы и системы мобильной коммерции могут быть выполнены как дополнительная опция, интегрированная в общую систему, в том числе и с АСУ и системой защиты от злоупотреблений.

Предлагаемое решение по системе оплаты проезда должно обеспечивать:

– всех основные платежно-информационные задачи, связанные с обслуживанием различных социальных групп;

– возможность восстановления данных при утере карты, учета истории для формирования льготных и бонусных программ, автоматизированный ввод данных для пассажиров имеющих федеральные и региональные льготы через «единое окно» на основе системы ЕСИА, совместимость с системой ЕПГУ и т.п.) и обеспечение привлекательности для пассажиров, в том числе межрегиональных и интермодальных пассажирских перевозок;

– возможность интеграции с системой управления НПТ и противодействия использования коррупционных схем оплаты проезда.

Горелик С.Л., Лещинский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПЕРЕВОЗКИ ПАССАЖИРОВ

Актуальность поставленной задачи обусловлена большим количеством эксцессов, наносящих вред здоровью пассажиров, других участников дорожного движения.

Основные причины высокого уровня аварийности:

1. Качество вождения:

– почти 50% аварийных ситуаций возникает из-за человеческого фактора;

– почти 30% технических неисправностей ТС являются следствием неправильного стиля вождения;

– почти 80% травм пассажиров в салоне обусловлены агрессивным стилем вождения, наличием неожиданных препятствий и т.п.

2. Техническое состояние транспортного средства:

– неисправности ходовой части приводят к аварийным ситуация с тяжелыми последствиями для пассажиров и других участников дорожного движения;

– неисправности двигателя и ходовой части являются наиболее частыми причинами нарушения расписания движения.

3. Состояние дорожной инфраструктуры:

– ровность дорожного покрытия;

– препятствия на пути движения (длительного действия и краткосрочные).

Задача повышения безопасности перевозки пассажиров активно решается в новых разработка АСУ НПТ второго поколения за счет использование систем предупреждения об аварийных ситуациях и террористической опасности, расширения функций мониторинга, использования технологии» «черного ящика», создания интеллектуальных систем для подготовки управляющих решений.

Для решения актуальных проблем осуществляется:

– внедрение новое поколение интеллектуальных бортовых устройств с расширенным перечнем функций, обеспечивающих предварительную обработку данных, адаптивное сжатие и передачу телематических информационных пакетов на процессинговый и диспетчерский центры;

– использование современных математических методов и алгоритмов для формирования информационных продуктов в интересах ОГИВ и широкого круга потребителей (страховых компаний, перевозчиков, служб экстренного реагирования и др.) на основе облачных технологий хранения и передачи данных.

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

ПРОБЛЕМА ПОСТРОЕНИЯ УМНОГО БЕЗОПАСНОГО ГОРОДА С ПОЛИЦЕНТРИЧЕСКОЙ СТРУКТУРОЙ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА

Большие города как правило возникают как системы с одним центром, по мере роста города моноцентризм становится тормозом в его развитии, порождая множество проблем –транспортных, демографических, промышленных, архитектурных. Решение этих проблем лежит на пути перехода к полицентрической структуре. Это ярко видно на примере Санкт-Петербурга, который до сих пор сохраняет моноцентрическую структуру, которая начала складываться еще со времен Петра Великого.В докладе обсуждает перспективная полицентрическая структура города, которая включает следующие центры : 1.Старый центр, истинный Санкт-Петербург. 2. Новое сити в районе Горской, где можно будет строить небоскребы и использовать аэродром в Левашово как деловой аэропорт. 3. Центр во Всеволожске. 4.Центр в Шлиссербурге. 5. Центр в Колпине. 6. Центр в Гатчине. 7. Центр в Бронке, будущий новый порт. Возникает много вопросов. Если говорить о Всеволожске и Шлиссербурге, то необходимо, чтобы город имел выход к Ладоге – главному резервуару пресной воды, чтобы правый берег Невы был в городе и можно было бы разместить новый зоопарк в Невском лесопарке, чтобы на Неве можно было построить две гидростанции – у истока Невы и в районе Ивановских порогов, чтобы лучше защитить город от катастрофических наводнений, которые предсказывают синоптики и с которыми существующая дамба не стравится. Если говорить о Гатчине, то это город с уникальными дворцовыми комплексами и институтами является органической частью Петербурга, а Ропшинские высоты являются источником водоснабжения фонтанов Петергофа. Город – сложная самоорганизующаяся человеко-машинная система, для управления которой уже давно необходимо использовать моделирование и компьютеры, но город – плохо формализованная система. Предлагается использовать лингво-комбинаторное моделирование для этой цели (см. книгу - Игнатьев М.Б. «Кибернетическая картина мира» СПб, 2014).

Лепёхин А.Н.
Республика Беларусь, Минск, Академия МВД Республики Беларусь

О НЕКОТОРЫХ МЕТОДАХ ОБРАБОТКИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Объективные предпосылки современного социума детерминируют изменения в преступной среде общества, порождая новые способы и методы совершения криминальных деяний. Более того, информационные процессы, сопровождающие указанные явления, обуславливают фокусирование внимания правоохранительных органов не только на фиксации противоправной деятельности и соответствующей реакции государства в рамках действующего законодательства по раскрытию и расследованию преступлений, но в первую очередь на профилактической, упреждающей деятельности органов правопорядка, направленной на реализацию превентивной функции соответствующих государственных органов. Очевидно, для качественной реализации указанных направлений деятельности правоохранительных органов необходимо соответствующее не только информационное, но и аналитическое обеспечение правоохранительной деятельности.

Более того, указанные трансформации преступной деятельности обуславливают необходимость совершенствования не только информационной, но аналитической деятельности, методов ее осуществления и выработке, на основе полученной и переработанной информации, управленческих решений соответствующими должностными лицами правоохранительных органов в целом, и органов внутренних дел в частности.

Следует акцентировать внимание, что в рамках информационно-аналитической работы необходимо смещать акценты ее осуществления с информационной составляющей (что также является важным) в сторону аналитического обеспечения реализации своих функций правоохранительными органами. Поскольку современные реалии таковы, что постоянно и многократно возрастают информационные потоки и объемы информации. К источникам такой информации можно отнести: сведения в различных ведомственных банках данных органов внутренних дел, данные, имеющие отношение к решению служебных задач, из автоматизированных банков данных других государственных органов, информация, образующаяся в процессе служебной деятельности органов внутренних дел (рапорта, справки, служебные материалы и др.), информация от других государственных органов, юридических лиц и граждан, сведения из средств массовой информации, в том числе, и размещенная в сети Интернет, а также другие источники.

Очевидно реализация функции и задач, возложенных на правоохранительные органы, и органы внутренних дел, в первую очередь, зависит от способности быстро и эффективно обработать, проанализировать указанные большие объемы информации и выдать конечный готовый продукт – оптимальное управленческое решение.

Решение данной задачи, по нашему мнению, невозможно без соответствующего научно-методического обеспечения, инструментария аналитического решения прикладных задач. И, в первую очередь, необходимо говорить о математических моделях и методах, позволяющих произвести операции отбора, ранжирования и верификации получаемой информации и продукта ее переработки – аналитических документов, и, соответственно, принятии на их основе решений тактического и стратегического характера.

В качестве приоритетных направлений применения математического аппарата для задач информационно-аналитического обеспечения деятельности правоохранительной деятельности следует выделить использование положений теории нечетких множеств и нечеткой логики, теории нейронных сетей, теории принятия решений, теории графов.

Анализ действующих подходов как в Республике Беларусь, так и в Российской Федерации к решению задачи информационно-аналитического обеспечения деятельности органов внутренних дел показывает, что аналитическая деятельность имеет, в основном поверхностный характер, заключающийся, в основном, в сравнении определенных показателей оперативно-служебной деятельности с предыдущим периодом, а также в проведении в ряде случаев факторного анализа и разработке регрессионных моделей, используемых в прогнозной деятельности.

Вместе с тем, следует отметить, что указанные выше методы не всегда могут быть эффективны и, соответственно получаемые результаты недостаточно достоверны, поскольку использование факторного анализа имеет ряд недостатков обусловленным наличием нелинейных статистических связей между наблюдаемыми переменными (факторами, влияющими на преступность). В таких ситуациях обоснованно использование положений теории нейронных сетей, поскольку нейронная сеть может выступить в качестве универсального аппроксиматора обучающих данных. Совместное использование моделей систем нечеткого логического вывода и нейросетевых моделей, которые сочетают в себе возможности сбора и обработки нечетких сведений (экспертных знаний о структуре объекта в виде лингвистических высказываний: если «входы», то «выход») и реализации способности возможности обучения сети на ограниченном множестве примеров.

При этом, как справедливо отмечается, что нейро-нечеткая сеть обладает двумя важнейшими человеческими (интеллектуальными) свойствами:

– лингвистичностью, т.е. использованием знаний на естественном языке;

– обучаемостью в реальном масштабе времени с последующим обобщением полученных знаний, что позволяет эффективно решить задачу управления в условиях информационной неопределенности в которых и складывается в основном деятельность органов и подразделений внутренних дел.

Таким образом, объективизация требований по совершенствованию информационно-аналитической деятельности требует качественно новых подходов к ее организации и проведении с учетом положений математической логики.

Присяжнюк С.П.,
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»

ПРИНЦИПЫ УПРАВЛЕНИЯ РЕГИОНОМ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОЙ ГИС

В докладе раскрывается опыт создания геоинформационных систем для управления регионами и территориями компании ЗАО «Институт телекоммуникаций». ГИС – это межведомственная система, которая объединяет в себе различные данные по территориям, моделирует развитие событий и предлагает варианты решения для реализации управленческого процесса. В докладе подробно освещены задачи и проблемы, возникающие перед управленческим аппаратом, способы и варианты их решения. Описываются различные модули для решения различных задач. Часть доклада посвящена техническим вопросам: структуре и архитектуре системы, порядку формированию баз данных и их вариантам. Более подробно раскрыты вопросы тематических слоев и их функций, приведено описание инструментария. В докладе подробно описан эффект от внедрения и использования подобных ГИС, приведены примеры реализованных проектов. Завершает доклад описание функциональных возможностей системы по моделированию ситуаций.

Присяжнюк С.П.
Россия, Санкт-Петербург, ЗАО «Институт Телекоммуникаций»

ГЕОИНФОРМАЦИОННАЯ ПЛАТФОРМА ДЛЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ РЕГИОНА

В современных условиях возрастания угрозы терроризма, изменения климата и социальной напряжённости обеспечение безопасности жизнедеятельности в регионах становится первоочередной задачей, решение которой требует согласованного комплексного подхода всех структур задействованных в решении данной задачи.

Интегрирующей основой является геоинформационная платформа для систем поддержки принятия решений по управлению регионом в чрезвычайных условиях.

В настоящее время в управленческих структурах используются радиообразные геоинформационные системы в основном импортного происхождения, что не позволяет создать единую геоинформационную платформу.

Предлагается отечественная геоинформационная платформа основанная на новейших технологиях с применением объектно-ориентированных моделей геопространственными данными и базы данных условных знаков оперативной обстановки.

По предметным областям используются базы знаний. Инструментальные геоинформационные средства совместимы с используемыми на практике форматами данных, что позволяет решить проблему импортозамещения и приемственности с наработанным геоинформационным ресурсом.

В платформе решены вопросы информационной безопасности при применении платформы в сетевом решении с возможностью использования мобильных предложений.

При разработке геоинформационной платформы учтен опыт создания геоинформационной системы 3D моделирования олимпийского строительства Сочи 2014 и разработки аналогичных систем для ряда регионов страны.

Степанов П.П.
Россия, Владивосток, Дальневосточный федеральный университет

АНАЛИЗ ПРОБЛЕМЫ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ

В настоящее время осуществляется процесс формирования системы электронного документооборота (СЭД) для внутреннего использования в структуре Администрации Приморского края. Информации, хранящейся и обрабатывающейся в СЭД, угрожает множество опасностей.

Документы могут быть утеряны по причинам ошибок в программном обеспечении, несмотря на ввод СЭД в эксплуатацию доработка интерфейсов и исправление ошибок продолжается, неграмотной работы пользователей, преднамеренной порчи данных и повреждения физических носителей. Риск потери данных существует всегда, так как абсолютная минимизации этих факторов невозможна. Сбои приводят к временному выведению системы из строя для проведения технического обслуживания, частота которых ставит под вопрос целесообразность внедрения подобной системы.

Общая для всех СЭД государственного назначения проблема – это стремительный рост объемов хранимых и обрабатываемых данных. Аналитики предполагают, что за период с 2015 по 2016 годы общий объем информации, циркулирующий в СЭД, увеличится в 1,5-2 раза. Соответственно, все серьезнее становится проблема надежного хранения данных и скорости доступа к ним.

В данном контексте традиционные системы становятся неэффективными, необходима оптимизация процессов жизненного цикла обрабатываемой информации, создание резервных копий и оптимизация процессов хранения.

Использование разработчиками свободно распространяемого инструментария для создания и модификации СЭД, приводит к повышению рисков целостности и конфиденциальности информации. Характерным примером является проблема «логического люка», не декларированной возможности доступа к системе в обход политики безопасности и правил разграничения доступа, создаваемой разработчиками для облегчения процессов интеграции, оперативности и удобства в решении задач по улучшению работы СЭД, оптимизации функционала и снижения задержек в процессе выполнения задач.

Естественный процесс закрытия подобных «люков» на этапе ввода в эксплуатацию в СЭД, интегрируемой в Администрацию Приморского края, не наступил, так как система до сих пор находится на стадии доработки. В результате, система может быть скомпрометирована, вследствие того, что технические учетные записи разработчиков имеют примитивные пароли.

Появление подобной проблемы – это результат действия совокупности факторов, приводящих к возможности злоумышленником сбора всеобъемлющего спектра данных, достаточного для формирования модели профессиональной парадигмы разработчиков. Следовательно варианты решения этой и следующих проблем безопасности, могут быть предугаданы злоумышленником с вероятностью, выходящей за зону «приемлемого остаточного риска». Учитывая критическую важность данной СЭД, даже закрытие данного «логического люка» ставит вопрос о смене команды разработчиков, для минимизации вероятности инцидентов безопасности в будущем.

В качестве первопричины аналитики выделяют недостаточное количество в структуре края ИБ-специалистов, а также сотрудников, ознакомленных с основами информационной безопасности, в том числе в составе разработчиков СЭД.

С подобной проблемой в 2011 году столкнулись в Хабаровском крае, IT департамент которого, на тот момент, включал лишь 6 специалистов в области информационной безопасности, а от создаваемой СЭД требовался дифференцированный доступ как к открытой, так и к закрытой части, с использованием как Web-интерфейса, так и отдельного приложения для портативных устройств. В результате предпринятых мер в IT департаменте, во-первых, число сотрудников, прошедших обучение в области информационной безопасности, увеличилось за три года до 134, то есть более чем в 22 раза, во- вторых, в качестве превентивной меры подобных инцидентов стало регулярным проведение киберучений, моделирующих атаки на нарушение конфиденциальности, целостности и доступности ресурсов края. Данная мера позволила уйти от чисто правовой защиты информации к программно-технической.

Томша П.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОЦЕНКА СТЕПЕНИ ВОВЛЕЧЕННОСТИ РЕГИОНАЛЬНЫХ ЗАКОНОДАТЕЛЬНЫХ ОРГАНОВ В РЕГУЛИРОВАНИЕ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нормативно-правовое регулирование области информационной безопасности в Российской Федерации осуществляется международными договорами и внутригосударственными нормативно-правовыми актами, основой для которых служит Доктрина информационной безопасности Российской Федерации.

Регионы имеют возможность самостоятельно регулировать сферу информационной безопасности в рамках федерального законодательства с помощью региональных законодательных органов. В данной работе представлена оценка степени вовлеченности региональных законодательных органов в процесс регулирования сферы информационной безопасности.

Для расчета оценки для каждого из регионов России был произведен подсчет числа действующих региональных законов, в которых используется термин "информационная безопасность". В качестве оценки мы приняли долю таких законов от общего количества действующих региональных законов, принятых законодательным органом в данном регионе.

Такая оценка отличается скоростью подсчета и предельной простотой и понятностью. Поэтому она может использоваться как индикатор для определения региональных особенностей в сфере регулирования информационной безопасности.

Термин "информационная безопасность" упоминается в 1,67% всех действующих региональных законов. По отдельным регионам этот показатель принимает значения от 0,46% до 5,18%.

Корреляция между общим числом законов в регионе и числом законов, связанных с информационной безопасностью, составляет 0,57, что не даёт нам права говорить о существовании линейной связи между данными показателями.

Больше всего внимания сфере информационной безопасности уделяется в Астраханской области, в которой доля региональных законов с упоминанием информационной безопасности составляет 5,18%.

Также значительное внимание регулированию сферы информационной безопасности уделяют Республика Крым и город Севастополь (доля региональных законов с упоминанием информационной безопасности – 4,56%), Карачаево-Черкесская Республика (4,39%), Новгородская область (3,57%), Курская область (3,5%), Республика Северная Осетия (3,49%), Московская область (3,22%) и Брянская область (3,04%).

Меньше всего внимания регулированию сферы информационной безопасности уделяется в Чукотском автономном округе, доля упоминающих информационную безопасность законов в которой составляет около 0,46% от общего числа региональных законов.

Значительно меньше среднего регулируют сферу информационной безопасности также Саратовская область (0,54%), Тюменская область (0,83%), Самарская область (0,84%), Республика Алтай (0,86%), Орловская область (0,87%), Челябинская область (0,88%), Томская область (0,88%), Ненецкий автономный округ (0,90%), Магаданская область (0,93%), Костромская область (0,94%), Амурская область (0,95%) и Республика Карелия (0,96%).

В остальных регионах доля региональных законов, упоминающих информационную безопасность, составляет от 1% до 3%.

Рассмотренная оценка помогает выявить регионы, имеющие обширный опыт регулирования сферы информационной безопасности посредством региональных законов.

В качестве рекомендации мы предлагаем регионам с высоким значением рассмотренной в данной работе оценки измерить эффективность регулирования сферы информационной безопасности на базе региональных законов и подготовить предложения по внедрению позитивного опыта в регионы с низким значением оценки.

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Алексеев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ АСПЕКТЫ ТЕХНОЛОГИИ СИНТЕЗА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА В ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

До настоящего времени законченной теории создания и применения автоматизированного рабочего места (АРМ) в составе подразделений органов внутренних дел (ОВД), при рассмотрении их как социальных организационно-технических систем (СОТС), включая формализацию процесса синтеза и оценку эффективности функционирования, не существует. Вместе с тем, на основании практического опыта наиболее устойчивая последовательность стадий синтеза АРМ нашла отражение в двух группах ГОСТ. Первая группа предполагает выполнение работы по созданию АРМ в форме опытно-конструкторской работы (ОКР), но не предъявляет к АРМ никаких специфических требований, рассматривая АРМ наравне с другими объектами технического синтеза. Вторая группа предъявляет более четкие требования к стадиям и этапам создания АРМ с учетом их специфики. Однако эти ГОСТы ориентированы на регламентацию синтеза относительно простых АРМ и не учитывают целый ряд особенностей АРМ в подразделениях ОВД, строящихся на принципах компьютерной сети (КС) и общего информационного ресурса (ОИР).

Как следствие этого, не предусматривается отработка системы на опытном образце и проведение испытаний (предварительных и государственных) опытного образца и комплекса средств автоматизации (КСА).

Согласно ГОСТ 2.103-68, в докладе выделены семь стадий разработки образца от аванпроекта до корректировки рабочей конструкторской документации (РКД) и доработки опытного образца (ОО) по результатам государственных испытаний. Вместе с тем, при такой организации не предусматривается выполнение ряда важных для качества синтеза работ:

1) на стадии разработки аванпроекта не предусмотрено:

– обследование органов управления объектом (объектами) с целью подготовки необходимых исходных данных для синтеза АРМ,

– выполнение научно-исследовательской работы (НИР) в обеспечение формирования технического задания (ТЗ) на АРМ в целом,

– выполнение технико-экономического обоснования на АРМ в целом;

2) на стадии эскизного проекта не предусматривается разработка и обоснование решений по эргономическому обеспечению проектирования АРМ;

3) на стадии разработки технического проекта не предусмотрено:

– выполнение обязательной разработки технических решений по созданию всех видов обеспечения (математического, программного, информационного, лингвистического) АРМ,

– наличие четкой регламентации вопросов макетирования КСА в целом и его составных частей.

4) не предусматривается также в качестве самостоятельной стадии ввод в действие созданного образца.

При этом настройка программного обеспечения по вводу нормативно-справочной и другой необходимой информации и подготовка операторского состава АРМ к организации опытной эксплуатации остаются вне поля зрения разработчиков системы, хотя требуют значительных временных и стоимостных затрат. Схема разработки АРМ в настоящее время установлена ГОСТ 24.601- 86. В докладе выделены ряд особенностей:

1. До стадии эскизного проектирования выполняются работы по исследованию и обоснованию создания АРМ в составе СОТС.

2. Формирование ТЗ на создание АРМ рассматривается как самостоятельный этап проектирования на стадии разработки эскизного проекта.

3. На стадии технического проектирования предусматривается получение самостоятельных решений по созданию видов обеспечения АРМ.

4. В качестве самостоятельной стадии рассматриваются работы по вводу АРМ в действие.

5. Учитывая сложность разработки программного обеспечения (ПО), оно может рассматриваться как самостоятельный объект проектирования.

Рассмотренные стадии и содержания работ «гостированной» технологии синтеза АРМ позволяют сделать вывод о том, что в качестве основных результатов синтеза можно принять: технический и экономический облики АРМ. Опыт последних десятилетий по синтезу и созданию АРМ различных классов показал сравнительно низкую эффективность реализации традиционной технологии, регламентированную стандартами групп ГОСТ. Это объясняется рядом причин:

1. Изменением свойств современных объектов синтеза, т.е. переходом от создания сравнительно простых закрытых АРМ в узких предметных областях управленческой деятельности к созданию интегрированных АРМ в составе СОТС ОВД и, следовательно, возрастанию масштаба и сложности решаемых в ходе синтеза задач.

2. Недостаточной степени регламентации ГОСТ таких стадий проектирования, как исследование и обоснование создания АРМ, разработка аванпроекта и эскизного проекта. Именно ошибки и недоработки, допускаемые на этих начальных стадиях проектирования, приводят к наиболее тяжелым случаям снижения качества создаваемой АРМ и, следовательно, к максимизации дополнительных затрат на их устранение в ходе опытной или даже реальной эксплуатации. На этих стадиях проектирования основными проблемами являются:

– формализация описания как структуры АРМ (в меньшей степени), так и процессов ее функционирования (в большей степени), являющихся объектами проектирования,

– спецификация функций лиц, принимающих решения, относительно подсистем АРМ и их органов управления,

– спецификация функций, выполняемых как персоналом, так и КСА или чаще всего совместно, обеспечение мобильности деятельности персонала АРМ, т.е. эргономическое обеспечение проектирования,

– спецификация потребностей пользователей (ЛПР, персонал управления) в части разработки эргономичных человеко-компьютерных интерфейсов в системе,

– спецификация профиля ГОСТ, положенного в основу создания АРМ.

3. Низким уровнем математизации методов, используемых на предпроектных стадиях разработки, которые не позволяют полно и однозначно описывать автоматизируемые процессы и функции управления, связывать их с современными информационными технологиями и прикладными платформами.

4. Отсутствием способов описания информационного и эргономического облика спроектированной АРМ с учетом их встраивания в действующую систему управления.

Следовательно, задача совершенствования с точки зрения информационной безопасности рассмотренных технологий синтеза сложных интегрированных АРМ в составе СОТС ОВД является важной и актуальной. Основные пути ее решения – это устранение рассмотренных четырех недостатков, главным образом за счет формирования полноценных информационного и эргономического обликов спроектированной АРМ.

Алексеев С.А., Горшкова Т.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ АСПЕКТЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ В ПОДРАЗДЕЛЕНИЯХ ОВД КАК СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМ

В составе подразделений органов внутренних дел (ОВД), практически все рабочие места начальников и руководителей подразделений, их заместителей и специалистов по направлениям являются АРМ, оснащенные средствами вычислительной техники с соответствующим программным и информационным обеспечением в виде набора стандартных пакетов и программ.Обобщенно, систему управления в подразделениях ОВД можно рассматривать, во-первых, как социальную систему, в состав которой входят как сотрудники руководства подразделений ОВД, отделов и секторов, так и персонал подразделений (социальные, хозяйственные подразделения и др.), которыми управляют. Во-вторых, подразделения ОВД вместе с объектами управления являются организационными системами, т.е. иерархическими системами с горизонтальными и вертикальными связями между ее компонентами. В-третьих, подразделения ОВД, сотрудники которых сами работают на АРМ и управляют подразделениями также оснащены рядом АРМ, является системой, в определенном смысле, технической, так как его персонал на всех уровнях управления использует средства вычислительной техники с соответствующим программным и информационным обеспечением. Таким образом, совокупность территориальных подразделений ОВД, решающих общую задачу, можно отнести к социальной организационно-технической системе (СОТС), относящейся к классу сложных, иерархических, самоорганизующихся и самоадаптирующихся человеко-машинных систем (ЧМС), в которых персонал управленцев работает на АРМ.

Проведенный анализ в территориальных подразделениях ОВД как СОТС показывает, что процесс управления таким сложным иерархическим объектом может осуществляться эффективно в случае, если все компоненты такой СОТС будут объединены в вычислительную сеть (ВС). Такая сеть является сетью передачи данных, в узлах которой располагаются ЭВМ и персонал, их использующий.

Фактически группа подразделений ОВД, связанных общей задачей, с точки зрения автоматизации управления, могут быть представлены в виде совокупности ЛВС.

ЛВС – это сеть передачи данных, связывающая ряд рабочих станций (рабочих мест операторов, АРМ, оборудованных средствами для выполнения функций управления) в одной локальной зоне. Такие сети обеспечивают высокие скорости передачи данных непосредственно в ЭВМ, подключенных к сети. Машины-шлюзы (межсетевые интерфейсы, служащие для соединения двух и более ЛВС, которые объединяют пользователей этих сетей) соединяют ЛВС между собой или подключают их к сетям большей протяженности. Каждая ПЭВМ в ЛВС имеет сетевой адаптер, который соединяет ее со средой передачи.

Для достижения определенных целей путем осуществления совместной деятельности на основе взаимных интересов система управления в территориальных подразделениях ОВД, может быть объединена, как с совокупностью подчиненных подразделений, так и с совокупностью подведомственных организаций в общую компьютерную сеть (КС). К любой КС предъявляются три основных требования:

– масштабируемость, позволяющая менять как число пользователей, работающих в КС, так и прикладное программное обеспечение,

– производительность, обеспечивающая пользователям работу с используемыми приложениями,

– управляемость, позволяющая пользователям перестраивать КС для удовлетворения потребностей в передаче данных.

Основными звеньями любой КС являются системные специалисты - операторы, рабочими местами которых являются рабочие станции или АРМ.

В докладе определены, что кроме операторского состава компонентами КС являются:

– коммутационные узлы – все сетевые устройства для соединения и объединения сети (повторитель, концентратор, коммутатор, маршрутизатор и др.),

– рабочие узлы (рабочие станции), оснащенные ПЭВМ, принтерами, сканерами, серверами и др.,

– каналы передачи данных, т.е. среда передачи информации (оптоволоконные, коаксиальные, радиоканалы и др.).

В настоящее время не существует отлаженной универсальной методики реализации мероприятий по синтезу, созданию и внедрению КС. Это связано с тем, что практически не существует двух абсолютно одинаковых организаций, представляющих собой СОТС. Каждая характеризуется уникальным стилем руководства, иерархией, правилами ведения дел (принятия решений). Любая КС в принципе должна отражать структуру организации, основой которой является персонал, работающий на своих АРМ. Каждый сетевой специалист-оператор должен осуществлять управление магистралью, которое включает: конфигурирование магистрали, поддержку ее работоспособности, передачу и прием сообщений. Следовательно, рассматривая подразделения ОВД России как СОТС можно представить их как разновидность ЧМС вида «группа операторов – корпоративная сеть» и использовать апробированные методы решения задачи информационной безопасности. Исходя из этого, при выборе технологии передачи данных в КС необходимо первым решать вопрос об обеспечении должной эффективности функционирования системы «группа операторов – корпоративная сеть», а затем о стоимости, скорости, перспективы расширения КС и поддержки существующей кабельной системы, обновления, входящих в нее технических и вычислительных средств, т.е. развития КС в соответствии с развитием организации СОТС,.

Бобонец С.А., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войскМВД России, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ ПРОЦЕДУР ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ

Одним из перспективных направлений защиты конфиденциальной информации в каналах связи можно считать создание и развитие компьютеризированных систем маскирования этой информации в речевых сообщениях наряду или при совместном использовании с традиционными технологиями смысловой защиты, а именно, засекречиванием речевых сигналов на основе криптографических алгоритмов.

Скрытие конфиденциальной информации в речевых сообщениях можно достичь только благодаря применению процедуры сжатия непосредственно речевых сигналов. Таким образом, применение той или иной процедуры сжатия диктуется не выбором соответствующего метода кодирования или записи сигнала, а способом представления аудиосигнала для восприятия слухом оператора с заданным уровнем качества. Решение этой задачи определяется как видно внутренними свойствами слуховой системы человека. Поэтому качество той или иной процедуры сжатия может быть оценено только экспериментально.

Такие эксперименты проводились на профильных кафедрах Санкт-Петербургского института внутренних войск МВД России и Санкт-Петербургского университета МВД России.

При проведении эксперимента предлагается использовать случайный механизм выбора сигналов для прослушивания. Все сигналы разбивались на два класса: неискаженных речевых сигналов и класс сжатых сигналов. Класс сжатых речевых сигналов разбивался на ряд уровней, каждому из которых соответствовала количественная характеристика, а именно, степень сжатия речевых сигналов. Данная количественная характеристика определялась относительной величиной фактически переданных отсчетов (слов) к исходному количеству отсчетов до процедуры сжатия.

Уровни качества оценки прослушиваемых сигналов задавались на основе данных предварительного психоакустического эксперимента.

Данные оценки вероятностей использовались в эксперименте в качестве меры эффективности предложенной процедуры сжатия сигнала.

Для контроля поступающей информации использовалась система – Spectralab – двуканальный анализатор спектра. Spectralab – это программа, которая реализует регистрацию и анализ сигналов в реальном масштабе времени. В основе функционирования программы положен алгоритм быстрого преобразования Фурье. Для математических расчетов и статистического эксперимента была привлечена программа MathCAD.

Решение поставленной проблемы – оценка эффективности разработанной процедуры сжатия речевых сигналов осуществлялась с помощью аудиометра нового класса, в котором были разработаны: специальная процедура консервации речевых сигналов с возможностью регулирования степени сжатия; процедура секционирования входных данных; алгоритм сжатия речевых сигналов с автоматической фиксацией ответных реакций; автоматического подсчета статистики эксперимента (создание файла статистики); изменения условий эксперимента (отношения сигнал/шум, параметров сигналов, количества представляемых сигналов в одном сеансе и т.д.); процедура оценка надежности экспериментальных данных.

На базе PC IBM созданы специальные программы, которые были, затем, включены в библиотеку математической среды MathCAD. Причина создания программ – указанная среда не имела согласования со звуковой картой компьютера, кроме того, в среде кроме операций ввода данных, а также запуска и остановки, отсутствуют функция «реакции» компьютера на ответы оператора (за исключением специальных команд), отсутствуют функции выдачи процедуры прослушивания сигналов, формируемой математической средой. Отсутствие этих операций не позволяло решить задачу алгоритмизации процедуры предъявления стимулов и подсчета ответных реакций оператора, т.е. реализации на компьютере функций стандартного аудиометра.

Новые возможности для психофизиологических исследований в данном аудиометре достигались за счет: возможности применения гибкой математической среды MathCAD при формировании классов сигналов и помех; достижения объективности оценки ответных реакций операторов за счет присутствия в методике случайного механизма выбора сигналов и моментов их предъявления; автоматической оценки надежности экспериментальных данных; контроля параметров сигнала, шума и отношения сигнал/помехи на математическом уровне; возможности использования аудиометра как тренажера обучения операторов.

Разработанная методика позволила провести эксперимент по оценке процедуры сжатия речевых сигналов, который помимо решения вышеуказанных задач доказал, что вейвлет-преобразование речевых сигналов является адекватной формой представления сигнала для слуховой системы человека.

Богданов С.Д., Стурза К.И.
России, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОДНО ИЗ НАПРАВЛЕНИЙ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

В сложившейся в настоящее время геополитической ситуацией связанной с введением в отношении Российской Федерации санкций со стороны США и стран Европейского Союза требуется переосмысление форм и методов достижения национальной безопасности нашей страны, и связанная с ними последующая корректировка комплекса мер направленных обеспечение национальной безопасности. Развитие мира идет по пути глобализации всех сфер международной жизни. Между государствами обострились противоречия, связанные с неравномерностью развития в результате глобализационных процессов, углублением разрыва между уровнями благосостояния стран. Национальная безопасность как система представляет собой совокупность связей и отношений, характеризующих такое состояние личности, общества и государства, при котором обеспечиваются устойчивое, стабильное существование, удовлетворение и реализация жизненных потребностей, способность к эффективному парированию внутренних и внешних угроз, саморазвитию и прогрессу.

В этих условиях усиливается, в том числе и глобальное информационное противоборство как между государствами (группами государств), так и в отношении крупных национальных или интернациональных компаний. Зачастую указанное противоборство связано с противоправной деятельностью в кибернетической области в форме хакерских атак на информационные базы, либо связанные с незаконным переводом (хищением) денежных средств. Информационный терроризм стал неотъемлемым атрибутом глобального информационного общества. Его можно считать проявлением крайнего экстремизма в информационной сфере, направленным на достижение политических целей через выдвижение отдельными лицами или организованной группой лиц требований к властным структурам, которые не могут быть удовлетворены в рамках существующего правового поля.

Информационная и информационно-аналитическая работ в сфере обеспечения безопасности осуществляется за счет управления системой информационных ресурсов органов государственной власти и государственных учреждений с использованием системы распределенных ситуационных центров работающих по общему регламента взаимодействия. В среднесрочной перспективе нам необходимо преодолеть технологическое отставание в области информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности, разработать и внедрить технологии информационной безопасности в системе государственного и военного управления.

Угрозы информационной безопасности России в ходе реализации «Стратегии национальной безопасности» должны предотвращаться за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности. Так, например, в военном направлении предстоит продолжать осуществление действий, препятствующих работе российских систем государственного и военного управления, обеспечению функционирования стратегических ядерных сил, предупреждению о ракетном нападении, противоракетной обороне, контролю космического пространства и обеспечению боевой устойчивости войск, действия, затрудняющие доступ России к стратегически важным транспортным коммуникациям и по другим сходным направлением.

Основное содержание обеспечения национальной информационной безопасности состоит в поддержании правовых и институциональных механизмов, а также ресурсных возможностей государства и общества на уровне, отвечающим национальным интересам Российской Федерации. При этом состояние национальной безопасности России напрямую зависит от экономического потенциала страны и эффективности функционирования системы обеспечения национальной безопасности. Реализация указанных выше направлений может обеспечиваться за счет консолидации совместных усилий и ресурсов органов государственной власти, институтов гражданского общества, направленных на отстаивание национальных интересов Российской Федерации путем комплексного использования политических, организационных, социально-экономических, правовых, специальных и иных мер разработанных в рамках стратегического планирования в Российской Федерации.

Большакова Л.В., Примакин А.И., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одной из задач информационной безопасности является задача принятия решения о выборе наилучшего варианта системы защиты информации в соответствии с имеющимся критерием. Системы защиты информации (СЗИ) имеют разные характеристики, по-разному действуют в различных ситуациях. Поэтому задачу выбора оптимальной СЗИ рекомендуется решать с использованием методов теории принятия решений. Специалист данной науки (или группа специалистов), называемый аналитиком или лицом, принимающим решение (ЛПР), обязательно учитывает условия, в которых должен происходить выбор. Эти условия позволяют классифицировать задачи теории принятия решений по ряду признаков.

По наличию имеющейся информации различают задачи принятия решений в условиях полной определенности, частичной или полной неопределенности.

ЛПР известны возможные угрозы и ответные действия каждой из систем, т.е. он знает насколько «хорошо» или «плохо» она действует в зависимости от вида возможной угрозы. Такая ситуация называется задачей принятия решений в условиях полной определенности. Как правило, такие задачи могут быть решены методами математического программирования, чаще всего, линейного. Эти методы позволяют выбрать оптимальный в соответствии с данным критерием, вариант из множества возможных решений.

ЛПР известны лишь вероятности возможных угроз и ответных действий на них каждой из систем. Такая ситуация называется задачей принятия решений в условиях частичной неопределенности или в условиях риска. Оптимальный вариант решения в таких ситуациях может быть найден, в частности, методами теории игр.

ЛПР ничего неизвестно о возможных угрозах или о возможных ответных действиях каждой из СЗИ. Такая ситуация называется задачей принятия решений в условиях полной неопределенности.

По наличию или отсутствию умного противника различают задачи принятия решений в условиях противодействия и без него.

Задачи принятия решения без противодействия не носят антагонистический характер, в них предполагается, что противник ЛПР не преследует никаких своих целей, реагирует на действия ЛПР беспристрастно, например, как природа. Для решения такого рода задач применяют конкретные критерии, например, критерии Вальда, Гурвица, Сэвиджа и т.д. теории статистических игр.

В задачах принятия решений в условиях противодействия имеется умный противник, который действует сугубо в своих интересах, как правило, противоположных интересам ЛПР. Противником в таких задачах может выступать конкурирующая фирма, военный представитель и т.д. Многие из таких задач могут решены методами теории матричных игр.

По числу целей различают одноцелевые (однокритериальные) и многоцелевые (многокритериальные) задачи принятия решений.

Методы математического программирования, теории матричных и статистических игр решают однокритериальные задачи, т.е. задачи, в которых оптимизация осуществляется в соответствии с одним определенным критерием.

На практике достаточно часто возникают задачи, в которых требуется принять решение, оптимальное сразу по нескольким критериям. Решение многокритериальной задачи состоит в преобразовании ее в однокритериальную с помощью процесса, называемого сверткой. Вначале применяют принцип Парето, согласно которому из рассмотрения могут быть убраны некоторые из допустимых решений, т.е. произойдет существенное сокращение размерности задачи. Оставшиеся решения образуют для данной задачи множество Парето. Далее вновь полученную многокритериальную задачу на множестве Парето сводят к однокритериальной с помощью введения некого обобщенного критерия. Этот обобщенный критерий является функцией от всех остальных критериев и носит название функции полезности.

По числу специалистов, выбирающих оптимальное решение, различают задачи принятия решений индивидуального и группового (корпоративного) выбора.

В задачах принятия корпоративного решения принимают участие несколько экспертов. В этом случае возникает ряд проблем, связанных с подбором группы экспертов, с выработкой согласованного решения и т.д. Такие проблемы решаются с помощью метода экспертных оценок.

Большакова Л.В., Примакин А.И., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Обеспечение защиты информации на практике происходит в условиях случайного воздействия самых разных факторов. Некоторые из них систематизированы в стандартах, некоторые заранее неизвестны и способны снизить эффективность или даже скомпрометировать предусмотренные меры. Тем не менее, оценка эффективности защиты информации должна обязательно учитывать эти объективные обстоятельства, а ее характеристики представлены в ГОСТ Р 51275-2006, который устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, с целью обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Представленное многообразие факторов предполагает системный подход и комплексную оценку уровня защищенности объекта, учитывая при этом целевое предназначение информационной системы. Такие исследования невозможно проводить без знания современных математико-статистических методов. Для исследования силы, вида и формы зависимостей широко применяются методы многомерного статистического анализа, которые позволяют выбрать ту вероятностно-статистическую модель, которая наилучшим образом соответствует исходным статистическим данным, характеризующим реальное поведение исследуемой совокупности объектов, оценить надежность и точность выводов, сделанных на основании ограниченного статистического материала.

Многомерный статистический анализ опирается на широкий спектр методов: множественный корреляционно-регрессионный, факторный, кластерный, дискриминантный, дисперсионный анализ, метод главных компонент.

Наиболее распространенными в практической работе в наше время являются методы множественного корреляционно-регрессионного анализа. При проведении системного анализа в многомерной совокупности эти методы позволяют оценить тесноту взаимосвязи между системами

показателей (факторов) и дать представление о стохастических связях между отдельной зависимой переменной и группой влияющих на нее факторов.

Часто в научных исследованиях возникает задача анализа неоднородных в некотором смысле данных. В таких случаях, прежде чем переходить к построению регрессионных моделей, необходимо выделить однородные группы объектов и уже внутри каждой группы строить регрессионные зависимости. Группировка первичных данных является основным приемом решения задачи классификации, а поэтому и основой всей дальнейшей работы с собранной информацией.

Методы кластерного и дискриминантного анализа предназначены для разделения рассматриваемых совокупностей объектов, субъектов или явлений на группы в определенном смысле однородные.

Наличие множества исходных признаков, характеризующих процесс функционирования объектов, заставляет отбирать из них наиболее существенные и изучать затем меньший набор показателей. Метод главных компонент и факторный анализ позволяют с минимальной потерей «сжать» информацию за счет некоторого преобразования исходных признаков, приводящего к уменьшению их числа. Они вскрывают объективно существующие, непосредственно не наблюдаемые закономерности при помощи полученных факторов или главных компонент, которые лаконично или более просто объясняют многомерные структуры.

Решение важнейших вопросов информационной безопасности на основе анализа множества количественных факторов, обеспечивающих эту безопасность, состоит из решения следующих основных задач методами многомерного анализа:

1. Проверка однородности множества факторов. В случае отсутствия однородности разделение этого множества методами кластерного анализа на однородные группы, пригодные для дальнейшего исследования.

2. Определение правила, по которому методами дискриминантного анализа может быть проведена классификация нового фактора и определена его принадлежность к одной из полученных кластер-групп.

3. Исследование методами корреляционного анализа наличия и силы внутри групповой или межгрупповой взаимосвязи между факторами.

4. Нахождение методами регрессионного анализа приближенной формулы зависимости одного фактора от других.

6. Выделение методами компонентного и факторного анализов главных факторов, влияющих на решение конкретной задачи, связанной с информационной безопасностью.

Большакова Л.В., Потехин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С КУРСАНТАМИ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 10.05.05 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ»

На кафедрах «Математика и информатика» и «Специальные информационные технологии» Санкт-Петербургского университета МВД России в соответствии с учебными планами подготовки курсантов по разным направлениям обучения, изучается ряд дисциплин, у которых практические занятия непосредственно связаны с применением информационных технологий. К ним относятся: математика, физика, основы информационной безопасности, программирование и др.

Так, в соответствии с тематическим планом дисциплины «Математика», курсантам необходимо освоить темы: «Основы линейной алгебры и дискретной математики», «Элементы математического анализа», «Элементы теории вероятностей и математической статистики». Данный материал требует от курсантов достаточно высокого уровня школьной подготовки по дисциплинам математической направленности. Однако, на практике уровень школьной подготовки курсантов не соответствует требованиям (к сожалению, при проведении вступительных испытаний, по дисциплине «Математика» экзамен не предусмотрен). В этом случае преподавателям кафедр необходимо довести уровень базовых знаний курсантов до требуемого, нейтрализовать сохранившийся у них после школы «страх» перед математическими задачами, которые, волей-неволей, им придется решать в процессе обучения. С учетом повышенного интереса у современных курсантов к инновациям, к компьютерной технике, как к средствам коммуникации и оперативного получения информации, как к чему-то новому, целесообразно использовать информационные технологии в процессе обучения для снятия психологического напряжения при необходимости решения математических задач.

Кафедрами отработана методика изучения математических дисциплин с применением интерактивного подхода на базе инновационных технологий, в частности, с использованием интегрированного пакета MathCad.

На сегодняшний день существует несколько математических пакетов, с помощью которых быстро, просто и эффективно выполняются сложные математические расчеты, причем даже в символьном виде. Здесь следует обратить внимание на такие средства вычислений, как Maple, Mathematica и Mathcad. Пакеты эти выделены именно потому, что в них на достаточно серьезном уровне поддерживаются символьные вычисления. Что касается пакета Mathcad, то в нем символьные вычисления являются скорее данью моде и ответом на современные вызовы рынка. Однако, это ни в коей мере не умаляет возможностей Mathcad, скорее наоборот. Он неизменно популярен, особенно среди студентов (курсантов) и инженеров (по-видимому, в силу простоты взаимодействия пользователя с приложением и прозрачности выполняемых операций). Возможности приложения постоянно расширяются, в силу чего Mathcad все чаще используется не только в физико-инженерных расчетах, но и при решении задач экономики, в финансовых расчетах, в социологии и биологии (список можно продолжить).

Методика сводится к выполнению курсантами предложенных заданий, предполагающих как расчет, так и символьные преобразования предложенных функций (при проведении дифференциальных и интегральных вычислений) с последующей проверкой результата в среде интегрированного пакета MathCad. При проведении практических занятий курсанты на первом этапе самостоятельно осуществляют решение задачи (без применения пакета MathCad), целесообразно, на этом этапе применять элемент «соревновательности», «соперничества» между курсантами. Первый, кто выполнит предложенное задание, имеет возможность, проверив его в интегрированном пакете MathCad, приступить к выполнению следующей задачи. Таким образом, при использовании данной методики налицо применение интерактивной технологии обучения: самостоятельное решение задач, проверка ее решения и переход к выполнению следующего этапа задачи.

Целесообразно применить вышеизложенную методику в процессе обучения курсантов, как под руководством преподавателя, так и в часы самостоятельной подготовки, что существенно повышает эффективность форм обучения.

Кроме этого, опыт проведения практических занятий с применением интегрированного пакета MathCad позволяет сделать вывод об эффективности освоения изучаемого материала при этом понимание «физики процесса» существенно повышается.

Интегрированный пакет MathCad позволяет визуализировать излагаемый материал. Например, в разделе «Основы математической статистики», понимание курсантами того, что такое «функция распределения случайной величины», «плотность распределения», какова связь между этими функциями, способ проверки полученного результата осуществляется достаточно оперативно и наглядно (в частности, нахождение площади фигуры под графиком плотности распределения, которая должна равняться единице, легко проверяется средствами интегрированного пакета MathCad посредством операции интегрирования указанной функции).

Таким образом, представленная выше методика применения инновационных технологий, интерактивный подход (теория – практика – теория) в процессе изучения вопросов математической направленности, позволяет эффективно достичь цели занятия – разобраться в достаточно непростых вопросах математического анализа основ статистики и применить их в практической плоскости.

Борисов А.А.Толкачева Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВАЯ ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ

Вопросы правового регулирования общественных отношений по поводу использования и распространения информации в целом и отдельных ее видов, в частности в последнее время, занимают одно из значительных мест в юридической литературе. Среди них, несомненно, много внимания уделяется проблемам правового регулирования банковской тайны.

Четкого определения банковской тайны в нормативных актах не дается, в том числе и в Федеральном законе «О банках и банковской деятельности». Российская банковская энциклопедия определяет банковскую тайну, как совокупность норм, устанавливающих перечень сведений, круг субъектов, обязанных обеспечивать сохранность, а также случаи и порядок доступа к сведениям, составляющим такого рода тайн.

В настоящее время миллионы людей пользуются услугами банков, такие как кредиты, вклады, операции с банковскими картами, платежи, переводы, инвестиции и ценные бумаги и др. Не задумываясь, клиент отдает этой организации свои персональные данные на обработку. Но как хранится и защищается личная информация неизвестно.

С одной стороны, банковская тайна защищает интересы клиента и запрещает, по общему правилу, доступ третьих лиц (в том числе государства в лице государственных органов) к конфиденциальной информации клиента банка. С другой стороны, нормы, регулирующие правоотношения, связанные с банковской тайной, закрепляют на законодательном уровне исключительные случаи и порядок такого доступа в интересах государства.

Необходимо относить к банковской тайне также сведения о личности клиентов, корреспондентов и лиц, упомянутых в контракте с банком. Это следует из того, что реквизиты клиента (корреспондента) также составляют содержание банковских операций и оформляющих их документов. Хотя, безусловно, предпочтительнее было бы сформулировать объем сведений, составляющих банковскую тайну, так, как это было сделано еще в Уставе Государственного банка в дореволюционной период –«хранить в тайне все, касающееся вверяемых банку частных коммерческих дел и счетов». Содержание права клиента на банковскую тайну составляют правомочие требовать от банковских служащих сохранения тайны и правомочие предоставить соответствующую информацию (часть ее) другим лицам. Справки по счетам и вкладам граждан выдаются, кроме самих клиентов и их представителей, судам и следственным органам по делам, находящимся в их производстве, если на денежные средства и иные ценности клиентов наложен арест, обращено взыскание или применена конфискация имущества.

Обязанность сохранения банковской тайны возложена законом на всех служащих банков независимо от их должности. Иногда банк в своих локальных актах дополнительно предупреждает об этой обязанности своих сотрудников. Так, в 1992 г. по приказу Центрального банка РФ его работники дали подписку о неразглашении сведений, связанных с деятельностью данного банка.

Нарушение банковской тайны состоит в раскрытии соответствующей информации (части информации) без согласия управомоченного лица (клиента, корреспондента) или в использовании ее банковским служащим в своих интересах. Такие действия могут причинить моральный, а иногда и материальный вред (например, в соответствии с полученной информацией похищена сберегательная книжка на предъявителя, государственная облигация и по ним получены деньги).

За вред, причиненный клиенту разглашением тайны, банк несет договорную ответственность в соответствии со ст.222 ГК РФ. Если банковская тайна раскрыта в отношении лица, не связанного с банком каким-либо договором (например, наследник, упомянутый в завещательном распоряжении банку), то наступает внедоговорная ответственность банка по правилам ГК (обязательства, возникающие вследствие причинения вреда).

В УК РФ нет статьи об ответственности за разглашение банковской тайны. Но возможно привлечение служащих к уголовной ответственности, если в их действиях содержатся составы предусмотренных в Кодексе преступлений, например, получение взятки за разглашение банковской тайны.

Буйневич М.В., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

КАТЕГОРИАЛЬНЫЙ АНАЛИЗ ПРОБЛЕМ ГАРМОНИЗАЦИИ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалистам в области информационной безопасности (ИБ), да и всем заинтересованным субъектам,сегодня невозможно обойтись без знания и исполнения требований соответствующей нормативно-правовой базы (НПБ). На то имеется несколько причин. Формальная состоит в том, что необходимость следования отдельным правилам и выполнять соответствующие требования закреплена законодательно со всеми вытекающими (в том числе, «репрессивными») последствиями. Однако наиболее убедительны содержательные причины. Дело в том, что НПБ это достаточно специфическая, но все же форма накопления и передачи знаний предметной области: вее документах зафиксированы апробированные, высококачественные решения и методологии по широкому спектру значимых вопросов.Далее, совместное безконфликтное сосуществование субъектов с разными интересамив инфосферев условиях нормативно-правового вакууманевозможно: недаром соответствующая Доктрина позиционирует нормативно-правовой уровень обеспечения ИБ сразу после морально-этического и духовно-нравственного. И наконец, международное и любое другое сотрудничество и/или взаимодействие при выполнении совместных работ и проектов в области ИБ без единой терминологической составляющей НПБ будет похоже на «строительство Вавилонской башни»: вот подтверждающее требование –«Установленные термины обязательны для применения во всех видах документации.Для каждого понятия установлен один термин. Применение синонимов термина не допускается» [РД. Защита от несанкционированного доступа к информации. Термины и определения. …Преамбула].

Проведенный авторами категориальный анализ современного состояния и тенденций развития НПБ ИБ позволил выявить ее следующие основные противоречия.

Во-первых, это устаревание vs обновление. С одной стороны, область ИБ является очень динамичной, что требует постоянного обновления НПБ. С другой стороны, руководящие документыdejure должны содержать сведения, полученные defacto в процессе «BestPractices».В качестве примера можно привести «галопирующую» модернизацию «Закона о персональных данных» от 2006 г. (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ,от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ,от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ,от 29.11.2010 № 313-ФЗ от 23.12.2010 № 359-ФЗ,от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ,от 05.04.2013 № 43-ФЗ, от

23.07.2013 № 205-ФЗ,от 21.12.2013 № 363-ФЗ, от 04.06.2014 № 142-ФЗ).В то же время, в этой очень переменчивой сфере, некоторые законы умудряются удерживаться по 15-20 и более лет: например «удачный» закон «О государственной тайне» от 1993 г.

Во-вторых, это количество vs качество. Сейчас только одним регулятором (ФСТЭК) в разделе «Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы…» и только по вопросамтехнической защиты информации зарегистрировано свыше 30 только открытых документов общим объемом 14304 kВили 1172 страницы (и это не считая свыше 60 стандартов по технической защите). О каком качестве освоения (прочтения, осмысления, согласования, а затем и внедрения в жизнь) этой НПБ можно говорить, даже если предположить высокое качество исходных документов (здесь уместно указать на возможные противоречия «профессионализм–дилетантство» и «объективность–субъективность» в отношении авторов). И это, когда не дан ответ на краеугольный проблемный вопрос необходимости vs достаточности(или избыточности) этого пуладокументов.

В-третьих, это мотивация vs стимулирование. Все усилия по разработке правильных и нужных правовых актов и руководящих документов окажутся тщетными, если они не будут применяться в каждодневной практике. Поэтому важнейшая задача – поиск способов стимулирования использования НПБ. Опыт отдельных компаний (правда, стран Евросоюза) показывает, что вложения в контроль исполнения НПБ может даже давать прибыль.

В-четвертых, всеобщность vs частность. Этопротиворечие проявляется в форме конфликта глобальных и национальных интересов в инфосфере, который находитсвое отражение в правовой плоскости. Важной проблемой здесь является гармонизация отечественной и международной НПБ, в частности, своевременные и качественные переводы нормативных документов, их обсуждение и согласование в русле общемировых тенденций, но не в ущерб информационному суверенитету. Ярким примером является выработка и принятие Модельного закона об информационной безопасности для стран СНГ.

Авторы пришли к выводу, что подавляющее большинство из выявленных противоречий не является антагонистическими, и, следовательно, тоже могут быть предметом согласования, гармонизации. Авторы считают, что научные исследования в направлении разрешения вышеуказанных проблемгипотетически позволят всем заинтересованным лицам, компаниям, научно-техническому сообществу и государствупозитивно повлиять на информационную безопасность через гармонизацию ее нормативно-правовой базы.

Васильков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПОЛИЦИИ» ОТ 7 ФЕВРАЛЯ 2011 ГОДА

В своей работе сотрудник Органов Внутренних дел всегда должен полагаться на нормативно-правовые акты, которые раскрывают вопросы не только основного вида деятельности сотрудника, но и моменты, связанные с обеспечением информационной безопасности граждан. В соответствии со статьей 17 Федерального Закона «О полиции» от 7 февраля 2011 года полиция:

1. Имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах (далее - банки данных).
2. Формирование и ведение банков данных осуществляются в соответствии с требованиями, установленными законодательством Российской Федерации.
3. Внесению в банки данных подлежит информация о различных лицах, указанных в законе.
4. Полиция обеспечивает защиту информации, содержащейся в банках данных, от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.
5. Информация, содержащаяся в банках данных, предоставляется государственным органам и их должностным лицам только в случаях, предусмотренных федеральным законом; правоохранительным органам иностранных государств и международным полицейским организациям - в соответствии с международными договорами Российской Федерации.
6. Полиция обязана обеспечить гражданину возможность ознакомления в порядке, установленном законодательством Российской Федерации, с содержащейся в банках данных информацией, непосредственно затрагивающей его права и свободы.
7. Обработка персональных данных осуществляется в соответствии с требованиями, установленными законодательством Российской Федерации в области персональных данных.
8. Персональные данные, содержащиеся в банках данных, подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Реализуя данную норму, полицейский обязан обладать навыками по созданию и ведению электронных банков данных. Информация, содержащаяся в банках, носит конфиденциальный

характер и имеет статус служебной тайны. Поэтому пункт 4 данной статьи возлагает ответственность на сотрудника полиции за обеспечение защиты данной информации от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.

Для обеспечения защиты государственной тайны, конфиденциальной информации полицейский должен обладать знаниями в области современных информационных технологий, использовать на практике достижения современной науки и техники, а также современную информационно-телекоммуникационную инфраструктуру (ст.11 ФЗ «О полиции»).

В пункте 7 Статьи 17 ФЗ говорится об установленных законодательством Российской Федерации норм в области персональных данных. Поэтому, в связи с обеспечением защиты конфиденциальной информации от утечки, полицейский должен обладать теоретическими и практическими навыками по своевременному устранению угроз безопасности и сведению к минимуму негативных последствий при их реализации.

Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ ПРОЦЕССА ОБУЧЕНИЯ КУРСАНТОВ ОСНОВАМ КРИПТОГРАФИИ

В органах внутренних дел уделяется большое внимание вопросам автоматизации, проектирования и программирования. Только за последние годы получены большие достижения в области, связанной с обеспечением безопасности конфиденциальной информации, сохранности секретных данных и сведений особой важности. Однако большая часть функций требуют преобразования и совершенствования. В особенности стоит вопроспо подготовке, особенно в правоохранительных органах, грамотных кадров и специалистов по вопросам связанным с этой областью.

После Второй Мировой Войны все разработки, связанные с криптографией во всех ведущих странах мира, были строго засекречены. В настоящее же время повсеместно стали обучать основам криптографии во многих высших учебных заведениях, не только за границей, но и в России,в связи со сложившейся обстановкой в нашей стране. Поэтому необходимо обеспечить совершенствование и создание новых систем шифрования, путем подбора, вербовки, обучения и подготовки талантливых кадров в секретные спецподразделения.

На сегодняшний день получены большие достижения в этой области, в частности, существует множество учебников по обучению основам криптографии, например курс лекций Г.В. Басаловой «Основы криптографии», в котором изложены основные подходы, методы и алгоритмы современной криптографии. Так же успешно используется учебник Н. Фергюсона и Б. Шнайера «Практическая криптография». Данная книга, написанная всемирно известными специалистами в области криптографии, представляет собой уникальное в своем роде руководство по практической разработке криптографической системы, устраняя тем самым досадный пробел между теоретическими основами криптографии и реальными криптографическими приложениями.

Однако проблема заключается в том, что вследствие развития современных персональных компьютеров, ЭВМ и мобильных устройств таких как: планшеты, смартфоны, ультрабуки, ноутбуки, электронные книги и т.д. удобнее, эффективнее и практичнее изучать системы шифрования представляется возможным с помощью программ устанавливаемых на персональный компьютер или на любые виды мобильных устройств. Учитывая данный факт, Британская спецслужба разработала мобильное приложение Cryptoy на мобильную операционную систему Android, которая успешно используется не только в высших учебных заведениях, но и в высших и профильных школах Великобритании. Проблема заключается в том, что даннуюпрограмму возможно эксплуатировать исключительно на иностранных языках, в связи с этим существует надобность создать аналог данной программы на русском языке. Так же в данной программе представлен узкий спектр систем шифрования, поэтому следует развить перспективную разработку представленной области и увеличить количество систем шифрования для обучения не только сотрудников ОВД Российской Федерации, но и сотрудников других структур и подразделений.

Именно в этой связи в рамках данной статьи предпринята попытка донести до читателя то, насколько важно развитие способов обучения сотрудников различных силовых ведомств и структур основным навыкам криптографической защиты информации за счет создания программных средств.

Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ЗНАЧЕНИЕ КРИПТОЛОГИИ ДЛЯ ОВД

В современном обществе несравненно возросло значение, количество и качество информационных систем и технологий, пронизывающих все сферы жизни общества, которые упрощают жизнь не только обычным гражданским, но и существующим на данный момент спецслужбам, министерствам и ведомствам, в том числе и Органам Внутренних Дел. В связи с этим

появились новые методы шифрования и дешифрования данных, чем, естественно, и занимается наука криптология.

Криптология как наука, изучает и разрабатывает научно-методологические основы, способы, методы и средства шифрования и дешифрования информации. Она же, равным образом, подразделяется на два основных направления, которые называются криптография и криптоанализсоответсвтенно.

Криптография – это наука, изучающая научные методы обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а так же невозможности отказа от авторства) информации.Криптоанализ же, в свою очередь, так же рассматривается как наука, только она изучает методы получения исходного значения зашифрованной информации, не имея доступа к секретным данным (ключу), а, иногда не имея доступа и к используемой системе шифрования. Кратко получается, что криптография – это наука, изучающая методы шифрования данных, то есть «защита», а криптоанализ – это наука, изучающая методы дешифрования данных, то есть непосредственно «нападение».

Криптосистемы, которые существовали до появления электронно-вычислительных машин, резко устарели,так как такой машине, которая могла быстро выполнять множество задач одновременно, не составляло труда расшифровать любые криптограммы тех времен. Для ОВДпоявилась необходимость шифровать данные, невидимые для злоумышленников, для передачи оперативной информации между Главным ИнформационнымЦентром Москвы, ИнформационнымЦентром Санкт-Петербурга и другими территориальными и региональными подразделениями, чем и занимаются нынешние криптографы, работающие на Органы Внутренних Дел.

Наряду с появлением компьютеров появился новый вид преступления, называемый киберпреступностью, к которому так же относится и передача зашифрованной информации по закрытым каналам, угрожающей безопасности страны. В то же время появилась необходимость раскрывать данные, шифрованные«киберпреступниками», чем собственно и занимаются криптоаналитики, но на данный момент техника быстро развивается, а нынешние системы и технологии шифрования и дешифрования данных, стоящие в подразделениях ОВД, к сожалению, мало используются.

Из вышеперечисленного следует вывод, что значение криптологии в связи с появлением и развитием электронно-вычеслительных машин для Органов Внутренних Дел достаточно велико. К сожалению, на данный момент системы шифрования и дешифрования данных мало распространены, но вместе с этим существуют и перспективы для повсеместного введения и использования в отделах МВДкриптографии для полного обеспечения засекречивания и безопасностилюбых видов секретных данных, а так же безопасности конфиденциальной информации.Так же существует надобность развивать криптоанализ, так как организованная преступность, а вместе с ней и киберпреступность, хорошо финансируется и оснащается необходимыми системами, а вследствие непрекращающегося развития и совершенствования информационных систем и технологий, системы стоящие на вооружении Органов Внутренних Дел с каждым днем устаревают.

Вождаев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

АНАЛИЗ ПРАВОВОГО ОБЕСПЕЧЕНИЯ РОССИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время, во всем мире, значительно возросло количествозаконодательныхколлизий, связанных с электронной экономикой. Все без исключения страны мира столкнулись с этой проблемой и сегодня стоят на пороге законодательных реформ в этой области. Намерения отдельных государств устанавливать законы в информационной сфере сталкиваются с технологической легкостью обхода вновь принимаемых законов.

В информационныхправоотношенияхпоявляются ранее неизвестные праву субъекты и объекты, методы информационно-правового воздействия, перестраиваются общепризнанные и появляются новые общественные отношения и связи. Вместе с тем, существует немалопробеловв правовом регулировании информационных процессов. Низок уровень правового сознания и правовой культурыюристов, практиков и научных работников, занимающихся проблемами защиты информации от несанкционированного доступа и обеспечения безопасности информации и информационной среды. Это наносит немалый ущерб структурам формирующегося в нашей стране информационного общества, деятельности всех участников информационного обмена и управления и прежде всего государства.

В нормативно-правовой базе федерального законодательства можно выделить:закон «О государственной тайне» от 21.07.93 г. № 5485-I;закон «Об обязательном экземпляре документов» от 29.12.94. № 77;закон «Об архивном деле в Российской Федерации» от 22.10.04. № 125;закон «О коммерческой тайне» от 29.07.04. № 98;закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 г. № 149;закон «О персональных данных» от 27.07.06 №152;закон

«Об электронной подписи» от 06.04.11 № 63 иряд.В целом они оказывают положительное влияние на состояние защищенности правовых интересов граждан Российской федерации в данной сфере. В то же время отдельные положения нормативных правовых актов российского законодательства, регулирующих отношения в области прав и свобод человека и гражданина, внутренне противоречивы и, в ряде случаев, не согласуются с нормами международного права.К числу наиболее серьезных недостатков правового обеспечения защиты прав и свобод человека и гражданина в информационной сфере следует отнести:

– Неопределенность механизмов обеспечения доступа к открытой информации органов власти, создающая условия для ущемления прав и свобод человека и гражданина.

– Отсутствие установленных норм ответственности за ограничение или нарушение права на доступ к открытой информации.

– Недостаточное правовое регулирование отношений в области сбора и использования персональных данных, механизмов их внесудебной защиты, реализации права на личную и семейную тайны, неприкосновенность частной жизни, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, телеграфных и иных сообщений.

– Недостаточную согласованность и полноту правовых норм, регулирующих установление режимов ограничения доступа к информации, обязанностей субъектов правоотношений по защите информации с ограниченным доступом, ответственности за нарушения установленных режимов ограничения доступа к информации.

– Слабое развитие правового регулирования отношений, связанных с ограничением массового распространения информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

– Отсутствие правового регулирования распространения информации, предназначенной для неограниченного круга потребителей, в открытых информационно-телекоммуникационных сетях.

– Диспропорции в развитии федеральной и региональной составляющей национального законодательства, наличие противоречий между ними, а также отсутствие законодательной базы для согласования законотворческой деятельности Российской Федерации и ее субъектов.

– Недостаточное правовое регулирование отношений в области развития технологического обеспечения информационной безопасности Российской Федерации.

– Недостаточная эффективность правовых механизмов установления ответственности за правонарушения в сфере обеспечения информационной безопасности.

Проведенный анализ состояния нормативного правового обеспечения информационной безопасности Российской Федерации позволяет сделать вывод о фрагментарности выбора объектов правового регулирования в области противодействия угрозам национальной безопасности в информационной сфере, недостаточной согласованности используемых для этого правовых механизмов, недостаточной эффективности, а, зачастую, и противоречивости используемых ими правовых норм.

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

СОВЕРШЕНСТВОВАНИЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННЫХ СЕКРЕТАХ

Законодательное регулирование не может обойти сферу защиты государственных секретов (государственной тайны), которая, отражаясь на степени открытости государства перед обществом, является важным и необходимым элементом обеспечения суверенитета и безопасности государства. В настоящее время базовые законы о государственных секретах (государственной тайне) приняты во всех государствах − участниках СНГ. Регулирование защиты государственных секретов в этих законах во многом сходно. Однако единый подход к определению государственной тайны, ее соотношению со служебной тайной не выработан. В национальных законодательствах государств – участников СНГ есть различия в подходах к законодательному определению категорий сведений, которые запрещено относить к государственной тайне, к предельным срокам засекречивания сведений и др.

Институт государственных секретов является национальным правовым институтом, однако активное сотрудничество государств – участников СНГ в различных сферах требует определённой международной унификации при установлении степеней и грифов секретности, единства подходов к пониманию ценности защищаемой государством информации. Это послужило основанием для принятия Межпарламентской Ассамблеей Содружества Независимых Государств (МПА СНГ) Модельного закона «О государственных секретах». Такой закон был принят в 2003 г. В Модельном законе государственные секреты подразделены на две составляющие их группы – государственную и служебную тайны.

За прошедшее десятилетие национальное законодательство государств в обсуждаемой сфере изменялось и совершенствовалось, модельное же законодательство СНГ на эти изменения никак не откликнулось. Сегодня в государствах – участниках СНГ имеют место четыре модели базовых законов, отличающихся своей терминологией и предметом правового регулирования. Это законы: «О государственной тайне» (Азербайджанская Республика, Российская Федерация, Республика Молдова и Украина); «О государственной и служебной тайне» (Республика Армения), «О государственных секретах» (Республика Беларусь, Республика Казахстан и Республика Таджикистан); «О защите государственных секретов» (Кыргызская Республика, Республика Туркменистан и Узбекская Республика) со своим предметом регулирования и понятийным аппаратом.

В 2010 г. Парламентская Ассамблея Организации Договора о коллективной безопасности (ОДКБ) приняла совместно разработанные научными коллективами России и Беларуси «Рекомендации по сближению законодательства государств – членов ОДКБ по вопросам государственной тайны».

Программой разработки проектов модельных законодательных актов и рекомендаций в целях сближения и гармонизации законодательства государств – участников СНГ на 2015-2016 гг. предусмотрена разработка Комментария к модельному закону «О государственных секретах». В настоящее время такая работа проводится. (Разработчиком был определён СПИИРАН, с учетом сложившейся кооперации с ИГПРАН и научно-исследовательскими институтами Республики Беларусь и имеющегося научного задела).

Проект разработанного Комментария к модельному закону «О государственных секретах» был рассмотрен на заседании Объединённой комиссии при МПА СНГ по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозами и направлен для получения экспертных заключений. Подготовленный интернациональным коллективом специалистов текст Комментария содержит обширный фактографический материал, который может быть использован при разработке дополнений в Модельный закон «О государственных секретах» и в работе над Рекомендациями по совершенствованию национального законодательства государств – участников СНГ. Такие работы инициированы Советом Федерации Федерального Собрания Российской Федерации и включены в раздел IV Перспективного плана модельного законотворчества в Содружестве Независимых Государств в области военного сотрудничества и безопасности на 2014 – 2016 гг.

Зайцева Е.А., Морозов Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

К ВОПРОСУ ОБ УГОЛОВНО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИЗА РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙГОСУДАРСТВЕННУЮ ТАЙНУ

Как известно, служба в силовых структурах всегда связана с различного рода информацией, в том числе,составляющей государственную тайну.

Для того чтобы рассматривать правовые аспекты, связанные с распространением государственной тайны, необходимо разобраться, что представляет собой государственная тайна.Федеральный закон «О государственной тайне» дает следующее её определение –это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. В данном определении указаны области государственной деятельности, в которых обрабатывается информация, разглашение которой может привести к угрозе национальной безопасности. Следует отметить, что в этом же документе содержится перечень сведений, которые отнесены к государственной тайне. Указ Президента РФ от 11.02.2006 N 90 «О перечне сведений, отнесенных к государственной тайне» конкретизировал эти сведения и сгруппировал ихпоследующим категориям:военная;экономика, наука и техника;внешняя политика и экономика;разведывательная, контрразведывательная и оперативно-розыскная деятельность.

Как видно из Указа, одной из разновидностей государственной тайны является военная тайна. Не вызывает сомнений тот факт, что разглашение военной, а равно и государственной тайны, всегда чревато тяжелыми последствиями для военной безопасности любого государства, поскольку влияет на боеготовность его Вооруженных Сил. Именно поэтому большое внимание уделяется правовой ответственности за посягательства на военную тайну. В данном аспекте представляется интересным рассмотреть ответственность за распространение информации, составляющейвоенную тайну.

Для сравнения, можно привести пример, как относятся к деяниям, связанным с разглашением государственной тайны,в Китайской Народной Республике:«21 января 2002 года Верховный суд КНР объявил, что, согласно новым законодательным актам, «кража, покупка или разглашение государственных и военных секретов через Интернет отныне приравнивается к государственной измене и карается смертной казнью». Впрочем, как уточняет агентство «Новый Китай», при наличии

тех или иных смягчающих обстоятельств смертная казнь может быть заменена на тюремное заключение сроком от 10 лет до пожизненного лишения свободы. Постоянный комитет Национальной народной ассамблеи опубликовал список преступных деяний, попадающих под новые правила. Наряду с прочими, в список вошли: проникновение на сайты государственных и военных учреждений и распространение электронных вирусов.

УК Республики Беларусь также имеет много отличительных особенностей по сравнению с УК РФ в области обеспечения защиты военной составляющей государственной тайны. Эти особенности заключаются в конструкции статей, и их структурном расположении в главах кодекса. Так, в главе «Воинские преступления» предусмотрены две статьи: за умышленное разглашение государственных секретов (ст. 457) и разглашение государственных секретов либо утрату документов, содержащих такие секреты по неосторожности (ст. 458). Отличительной особенностью этих статей, является то, что предметом преступления здесь являются сведения, составляющие государственную, или служебную тайну.

УК Украины, по сравнению с УК РФ, в части рассматриваемой темы, также отличается совершенством, поскольку сохранил приоритеты в области защиты военных секретов. В специальной главе о воинских преступлениях, предусмотрена статья 422, устанавливающая ответственность любого военнослужащего за разглашение сведений военного характера, составляющих государственную тайну. Причем, не имеет значения, были они доверены военнослужащему, или стали известны в связи с выполнением служебных обязанностей, - ответственность наступает в любом случае.

Отличительной особенностью УК Латвийской Республики, по сравнению с УК РФ, является то, что опираясь на богатейший опыт законодательства советского периода, в нем предусмотрена ответственность за разглашение военных сведений, не составляющих государственную тайну, но не подлежащих оглашению (ст. 352). Интерес также представляет статья 330 УК ЛР, предусматривающая ответственность за разглашение сведений, не подлежащих оглашению, после оставления должности. По всей вероятности, это относится и к военнослужащим ушедшим в отставку, на пенсию, или перемещенным по службе.

Анализируя уголовное законодательство некоторых европейских стран, можно прийти к выводу, что в экономически развитых, и политически стабильных западных государствах, охране государственных и военных секретов придают немаловажное значение.

Уголовно-правовая ответственность за посягательство на военную составляющую государственной тайны и другие военные сведения конфиденциального характера предусмотрена в уголовных кодексах многих зарубежных государств. Анализируя данные нормы, можно прийти к выводу, что в экономически развитых и политически стабильных западных государствах охране государственных и военных секретов придают немаловажное значение.

Законодательное определение ряда правонарушений, совершаемых военнослужащими, обусловлено особенностями порядка прохождения ими военной службы.

В настоящий момент за разглашение и утрату документов или предметов, содержащих государственную тайну, военнослужащие несут уголовную ответственность в соответствии с Уголовным кодексом РФ на общих основаниях. Аналогичные деяния, совершаемые ими в отношении военной тайны (военных сведений конфиденциального характера, не подлежащих оглашению), в настоящий момент остаются безнаказанными. Очевидно, что такое положение не соответствует требованиям ФЗ «О статусе военнослужащих».

Правовая неопределенность в вопросах ответственности военнослужащих за преступления, повлекшие разглашение военной тайны или утрату документов, либо предметов ее содержащих, может привести к ряду негативных последствий. Для Вооруженных Сил России они могут быть самыми катастрофическими. В ближайшем будущем армия может оказаться в принципе небоеспособной, поскольку, как организация, о структуре, работе и личном составе которой станет известно практически все: от дислокации и предназначения личного состава до социально-психологического портрета каждого военнослужащего.

За это гражданин, равно как и военнослужащий может быть осужден по четырем статьям УК РФ в случае нарушения им режима государственной тайны:

– Ст. 275 УК РФ«Государственная измена». Наказание: от 12 до 20 лет заключения, плюс штраф до 500000 рублей.

– Ст. 276 УК РФ«Шпионаж». Наказание: лишение свободы от 10 до 20 лет.

– Ст. 283 УК РФ«Разглашение государственной тайны». Наказание: лишение свободы до 4 лет, в особых случаях - от 3 до 7 лет.

– Ст. 284 УК РФ«Утрата документов, содержащих государственную тайну». Наказание: лишение свободы до 3 лет.

Таким образом, разглашение государственнойтайны влечёт за собой уголовная ответственность поэтому, с военнослужащими необходимо проводить ряд мероприятий по предупреждениюи профилактике преступлений в области государственной (военной) тайны.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРАВОВЫЕ АСПЕКТЫ ПОСТРОЕНИЯ WEB-САЙТОВ

Сегодня особого разговора заслуживает такой вид информационных технологий как Интернет-сайт. На страницах Интернет-сайта можно не только размещать информацию различных типов, но, и использовать специально разработанные программы, позволяющие организовать активное взаимодействие с пользователями, в том числе в реальном времени. Именно возможность организации обратной связи и является основным отличием и преимуществом Интернета перед другими медиа-средствами.

При ведении Интернет-сайта правомочным становится главный вопрос – а является ли сайт объектом авторского права. Ст. 1225 ГК РФ, прямо не выделяя сайт как объект авторского права, позволяет исследователям высказывать различные точки зрения по данному поводу.

Например, в работе М. Каранда сказано, что сайт не относится к объектам авторского права на том основании, что он не является ни компьютерной программой, ни базой данных, а законодательством охраны подобного рода высокотехнологического продукта не предусмотрено. То есть, ни под какую из существующих категорий произведений авторского права он не подпадает, а специально, как разновидность объекта авторского права законом он также не признан.

Но документ Интернета (каким можно считать Интернет-сайт) сам по себе имеет все признаки произведения и (в значительной степени) может быть объектом авторского права. Поэтому было бы неверным в качестве особого объекта сетевых отношений признавать только сайт в целом, т. к. это может привести к нарушению прав авторов документов Интернета.

Есть сторонники признания сайта базой данных. Хотя такой подход правомерен, но на практике он мало что дает, поскольку цель признания особых прав у составителя сборника (каким можно считать базу данных) – защитить его творческие усилия, а не подменить права на объекты, включенные в сборник.

Однако ряд авторов однозначно относят сайт к числу объектов авторского права. Используя формулировку ст. 1225 ГК РФ, в частности словосочетание “другие произведения” сторонники данной точки зрения считают, что, поскольку перечень объектов авторского права не является исчерпывающим, сайт может быть признан объектом. Во всяком случае, к указанным в ГК РФ произведениям, не являющимся объектами авторского права (перечень исчерпывающий), он никак не относится.

В работе А. Серго приводится мнение Министерства Российской Федерации по делам печати, телевидения, радиовещания и средств массовых коммуникаций, которое касается авторского права в Интернете. Авторская работа, размещенная на сайте в Интернете, является объектом авторского права, если является произведением в смысле ст. 1225 и 1255 ГК РФ, т.е. соответствует перечню объектов авторского права, является обнародованной или необнародованной, но находящейся в объективной форме. Следовательно, электронная статья является объектом авторского права. При этом размещение авторской работы на сайте в Интернете является обнародованием, поскольку делает произведение доступным для всеобщего сведения. Отсюда следует, что, если статья, размещенная в Глобальной сети, признается объектом авторского права, то и сайт, в качестве места размещения статьи, по всей вероятности, тоже должен признаваться объектом авторского права.

Таким образом, можно говорить о том, что хотя законодательно сайт не является объектом авторского права, практика относит его к данной категории. Соответственно автор сайта, как любого другого объекта авторского права будет обладать личными неимущественными и имущественными правами.

По нашему мнению, исходя из приведенного выше определения объектов авторского права, которыми являются произведения науки, литературы и искусства, находящиеся в какой-либо объективной форме (в частности, в электронной), сайт является объектом авторского права. Однако следует подчеркнуть, что поскольку сайт законодательно не относится к объектам авторского права, то свои авторские права автору сайта следует отстаивать в суде.

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРАВОВЫЕ ОСНОВЫ ОРГАНИЗАЦИИ ИНТЕРНЕТА

Сегодня благодаря постоянному расширению глобальной сети и ее возможностей Интернет становится основной экономической составляющей строящегося информационного общества.

Возникнув как средство для обмена информацией, в настоящее время Интернет представляет территорию, на которой активно продают и покупают, рекламируют и оплачивают товары и услуги, пользуются возможностями интернет-банкинга и голосуют и т.п. Интернет дает массу возможностей по развитию существующих коммуникаций, обеспечивает мощную и быструю обратную связь

компании-производителя и потребителя, позволяет решить проблему больших расстояний и значительно уменьшить финансовые затраты при обеспечении коммуникаций. Появление Интернета дало огромный толчок инновациям в области продвижения продукта, привело к скачку на рынке товаров и услуг. Поэтому правовые аспекты, связанные с его развитием и применением, являются чрезвычайно актуальными.

В связи с проблемой правового регулирования Интернета возникают следующие основные вопросы:

– является ли Интернет сферой, которую необходимо регулировать нормами права, какова вообще правовая природа данного явления?

– допустимо ли вмешательство государства в отношения, возникающие в связи с использованием Интернета, и, если да, то в каких пределах, как разграничить юрисдикцию различных государств применительно к таким отношениям?

– каково должно быть соотношение в нормативном регулировании Интернета издаваемых государством общеобязательных правовых норм и саморегулирующих норм сетевого сообщества (норм сетевого этикета)?

Интернет с точки зрения участниковИнтернет-сообщества представляется как уникальная информационная среда, характеризующаяся следующими признаками:

– не является ни средством массовой информации в его законодательном понимании, ни аппаратным средством связи, он представляет собой уникальную среду межличностного общения, имеющую наднациональный, надгосударственный характер;

– не имеет собственника, не принадлежит какому-либо государству, организации либо физическому лицу;

– доступ к ресурсам является частным правом граждан и не может быть ограничен путем установления государством каких-либо административных барьеров, препятствующих в той или иной мере его свободному использованию (лицензирование доступа, цензура содержания интернет-ресурсов и т.п.);

– является полностью саморегулируемой информационной средой, пользователи которой самостоятельно определяют правила поведения.

В последнее время все чаще признается, что единственной возможной и разумной целью регулирования отношений, связанных с Интернетом, является приспособление действующего законодательства к «реалиям виртуальной жизни», например, законодательства о средствах массовой информации, гражданского и гражданского процессуального законодательства, законодательства о конкуренции.

Законодателем предпринимаются попытки определить место государства в системе отношений, возникающих в Интернете, теоретически и практически решить проблему обоснования юрисдикции государства применительно к отдельным правилам, сделкам, правонарушениям, возникающим в связи с использованием Интернета.

Однако, отношения, возникающие в связи с использованием Интернета, весьма часто невозможно привязать к какой-либо территории и, следовательно, к какому-либо правопорядку.

Представляется целесообразным сочетание государственного регулирования и общественного самоуправления с соблюдением следующих принципов:

– обеспечение прав и свобод граждан, установленных конституцией;

– учет особенностей построения и развития сети Интернет, включая применяемые технические и организационные нормы и правила, а также сложившиеся в сообществах операторов и пользователей сети правила и обычаи, не противоречащие законодательству государства;

– нераспространение методов правового регулирования на организационные и технологические аспекты развития и функционирования сети, а также на аспекты, затрагивающие права и интересы личности, общества и государства.

Макарова Е.Н., Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

К ВОПРОСУ О ПРАВОВОМ ОБЕСПЕЧЕНИИ КОНТРОЛЯ СЕТИ ИНТЕРНЕТ В РОССИИ

Вопрос о том, кто и как должен контролировать и определять условия международного информационного обмена посредством сети Интернет, нужен ли такой контроль в принципе, и какова будет его эффективность в настоящее время весьма актуален. Сформировалось два основных подхода к его решению: одни ученые считают, что Интернет – единое информационное пространство всего мира, в котором государственные границы стираются, и для решения связанных с ним проблем необходимо международно-правовое регулирование телекоммуникационного пространства; вторые (и их большинство) полагают, что суверенитет над национальным сегментом Интернет принадлежит той стране, на территории которой этот сегмент размещается. Если это российский сегмент – то соответственно за Россией и т.д.

Сейчас около двадцати стран мира имеют зачатки национального законодательства, относящегося к регулированию сети. Спорных ситуаций в связи с использованием Интернет становится все больше, постепенно формируется судебная практика, которая показывает, что суд в большинстве случаев исходит из верховенства национального законодательства над информационными отношениями, если потребитель информации находится под юрисдикцией конкретного государства или штата. В России в настоящий момент, такая судебная практика, к сожалению, весьма невелика.

Во всем мире национальное законодательное регулирование Интернет осуществляется на основании одного из двух подходов. В соответствии с первым из них Интернет является совершенно новой технологической реальностью, которая требует принятия совершенно новых законов – так, космическое право появилось после запуска первых искусственных спутников Земли. Согласно другой точке зрения, Интернет – всего лишь еще одна среда, в которой сохраняются те или иные привычные правоотношения, поэтому нет необходимости изобретать специальные законы «Об Интернете», достаточно, чтобы действующее законодательство учитывало особенности этой среды. Россия до сих пор окончательно не определилась, по какому же пути идти: существуют и многочисленные попытки принять всеобъемлющий закон, касающийся Интернет, а наряду с этим различные нормативные акты дополняются поправками, относящимися к глобальной сети. Таким образом, правовая база Российского Интернет-пространства крайне мала и противоречива, а большинство вопросов и ситуаций попросту не имеют законодательного закрепления.

Морозов Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ НЕСЕРТИФИЦИРОВАННЫХ СРЕДСТВ СВЯЗИ В СИЛОВЫХ СТРУКТУРАХ

Мобильные телефоны, смартфоны и карманные компьютеры стали верными помощниками человекукак в работе, так и в привычных офисных условиях, а также в более агрессивной среде. Самой агрессивной (во всех смыслах) средой по праву можно назвать силовые, военные и правительственные ведомства.

Несмотря на свои военные корни, сотовая связь в силовых структурах появилась лишь недавно, да и то отношение к ней и по сей день довольно спорное. На то есть ряд причин. Во-первых, некоторая ненадежность. Возможность прослушивания разговоров и отслеживания сигнала является неотъемлемым плюсом в борьбе с неблагонадежными лицами с одной стороны, и крайне нежелательна для самих спецслужб с другой. Выходом может стать лишь повышенная степень защиты, которая есть лишь у избранных моделей. Во-вторых, доступность. При сегодняшнем распространении сотовой связи, за ней довольно сложно уследить, а потому это повышает риск промышленного и политического шпионажа, что стало особенно актуально с появлением мобильных телефонов со строенными цифровыми камерами. Отсюда запрет на пользование сотовыми аппаратами, например, в тюрьмах, в армии, особенно во время военных действий. В-третьих, нестабильность. При определенных условиях (например, в чрезвычайных ситуациях), сети могут оказаться перегруженными, что может не позволить профессионалам воспользоваться сотовой связью во спасение жизни людей. Такая ситуация, в частности сложилась во время террористических актов 11 сентября в США, что способствовало разработке особой системы доступа к мобильной связи спецслужб США. Эти, казалось бы, незначительные для повседневной жизни и обыденного пользователя факторы не позволяют назвать сотовую связь идеальным решением для работы в чрезвычайных ситуациях и во время военных и контр террористических операций. Тем не менее, она используется. С некоторыми ограничениями, оговорками, но используется. Причем, использование ее двухстороннее. С одной стороны извлекаются выгоды из эксплуатации коммерческих сетей, с другой, существуют специальные решения и устройства для успешной работы и координации действий специальных ведомств.

В настоящее время Министерством внутренних дел России, а так же Главным командованием внутренних войск МВД России выпущен ряд нормативно-правовых документов, запрещающий военнослужащим пользоваться сотовой связью, равно как и другими радиопередающими и радиопринимающими устройствами (радиоприёмником, wi-fi роутером, 3g модемоми др.). Только вот некоторые требования с этим запретом очень сильно расходятся.

Первое требование командиров –военнослужащий должен быть всегда на связи, в любое время дня и ночи, где бы он ни находился. В воинской части и солдат, и офицер находится почти 12 часов в сутки – это если усреднить. Как было указано выше, мобильной связью в силовых структурах, а в частности и во внутренних войсках, пользоваться нельзя.За использование телефона могут привлечь к дисциплинарной ответственности от строгого выговора до лишения допуска к секретной информации с последующим увольнением с военной службы.Офицерам же, командирам подразделений, старшие начальники приказывают изымать телефоны у личного состава, нельзя же

как бы, приказ запрещает, в то же время они же и наказывают офицеров за то что они не на связи.В данном аспекте можно увидеть очень много разногласий между командирами и подчиненными.

Одним из очевидных решений для того, чтобы максимально устранить недостатки сотовой связи в служебных целях – создание собственной сети, работающей на частотах, недоступных простому смертному. Однако это решение довольно дорогостоящее, да и, к тому же, не сильно отличается от привычных раций. Кстати, во время спец. операций бойцы отрядов специального назначения продолжают использовать для координации действий именно этот вид связи как наиболее безопасный. Да и вообще рации пока незаменимы в полиции и армии. А набирающая обороты технология PushtoTalk (нажми и говори), по сути, превращает обыкновенный сотовый именно в рацию. Что же касается аппаратуры, то при преимущественном доступе к существующим сетям, для повседневной связи и работы спецслужб, вполне подойдет массовый аппарат, который может удовлетворить требованиям военных. Наиболее ярким примером такого сотового телефона является Nokia 6340.

Таким образом, можно сказать, что запрещение сотовой связи в силовых структурах, а в частности и во внутренних войсках, не всегда влияет благоприятно, а иногда даже наоборот. Поэтому необходимо решать данную проблему, чтобы извлечь максимум выгоды от использования сотовой связи и сохранения коммерческой тайны и обеспечения экономической безопасности.

Нигметов Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВОПРОСОВ БЕЗОПАСНОСТИ СОДЕЙСТВИЯ ГРАЖДАН ОПЕРАТИВНО-РАЗЫСКНЫМ ОРГАНАМ

Для того чтобы говорить о содействии граждан оперативно-разыскным органам (ОРО), следует дать понятие термину «содействие», а также определить его соотношение с термином «сотрудничество», так как оба эти понятия используются в ныне действующем законодательстве в сфере оперативно-разыскной деятельности (ОРД).

Содействие граждан ОРО – это осознанное волевое поведение лиц, заключающееся в получении оперативно значимой информации и передачи её представителю ОРО, или осуществление конкретных действий по решению оперативно-разыскных задач борьбы с преступностью по инициативе ОРО при условии доверительности и при необходимости конспиративности отношений.

Этот термин включает в себя не только сбор и передачу лицом информации, но и его участие в подготовке оперативно-разыскных мероприятий, а также в их реализации, в предупреждении совершения конкретных преступлений.

Обычно содействие граждан ОРО осуществляется с помощью негласных методов и средств оперативно-разыскной деятельности. Это объясняется тем, что в сплоченной криминальной среде, в том числе в организованных преступных формированиях (ОПФ), считается неприемлемым оказывать содействие правоохранительным органам, а потому факт наличия контактом между представителем преступного мира и сотрудником ОРО, ставший известным в криминальной среде, может серьезно навредить безопасности лица, оказывающего содействие.

Следовало бы также обратить пристальное внимание на употребленный в вышеприведенном определении термин «доверительность отношений». Уровень доверительности отношений в процессе содействия граждан ОРО играет очень важную роль. Следует четко представлять опасность, которую, как и для содействующего лица, так и для сотрудника ОРО представляет работа по борьбе с преступностью, особенно с организованной. И от того, насколько верно оперативный работник определит степень доверия, которую он сможет оказывать тому или иному лицу, зависит жизнь не только самого сотрудника, но и содействующего лица.

Чтобы определить соотношение терминов «содействие» и «сотрудничество» следует обратиться к определениям, которые даны в Толковом словаре русского языка. В данном источнике термин «содействие» определяется как «совместное действие, соучастие; помощь, поддержка в чем-либо», а термин «сотрудничество» как «участие в каком-либо общем деле или же совместные действия, деятельность».

Исходя из этого, можно сделать вывод, что термин «содействие» является более емким, чем термин «сотрудничество».

Поэтому принято считать, что первый термин следует употреблять в отношении всей сферы содействия граждан ОРО, а второй – исключительно к содействию граждан на контрактной основе.

Выделяют несколько видов содействия граждан органам, осуществляющим ОРД:

– гласное содействие: заключается в открытом участие лиц в подготовке и проведении ОРМ. Данный вид содействия часто используется внештатными сотрудникам полиции, дружинниками, специалистами, переводчиками;

– анонимное содействие: заключается путём предоставления ОРО оперативно значимой информации, если лицо не желает раскрывать свое имя, а также впоследствии участвовать в уголовном процессе;

Желание лица сохранить анонимность может быть вызвано разнообразными причинами: причастность к криминальной среде, нежелание раскрытия степени своей осведомленности перед кем-либо, недоверие правоохранительным органам. И в любом из этих случаев оперативному работнику категорически запрещается склонять анонима к раскрытию своих личных данных.

Негласное (конфиденциальное) содействие: заключается в оказании гражданами (конфидентами) добровольного содействия ОРО с условием сохранения конфиденциальности лица. Данный вид содействия наиболее распространен и предполагает, что оперативный работник знает определенные сведения о лице, которое содействует ОРО, однако не имеет права разглашать эти сведения.

Привлечение к содействию граждан – одно из направлений деятельности ОРО. В ныне действующем законодательстве в сфере ОРД используются термины «содействие» и «сотрудничество». Термин «содействие» включает в себя понятие «сотрудничество», так как сотрудничество с ОРО подразумевает под собой наличие контракта. Существует три вида содействия: гласное, анонимное и конфиденциальное, последнее наиболее распространено. Привлечение граждан к содействию является наиболее эффективным методом борьбы с преступностью на современном этапе развития общества.

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ОСНОВА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

В последние годы развития человечества быстрыми темпами происходит информатизация общества – осуществляется постепенный переход от индустриального общества к информационному обществу. В информационном обществе владение информацией и всеми методами, формами и средствами ее производства, распространения, хранения, обработки и использования – это объективная необходимость для каждого члена общества.

В июле 2014 года президентом Российской Федерации Владимиром Владимировичем 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 России, хранить персональные данные граждан РФ только на серверах, расположенных на территории нашей страны.

С 1 сентября 2015 г. 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, 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 этого 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. Если буквально толковать законы, то мы увидим, что блокировке будут подлежать сайты «содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных».

Другими словами, речь идет о сайтах, которые содержат персональные данные. К таким сайтам могут относиться небезызвестные «базы данных граждан России онлайн», «телефонные книги» и другие сайты, которые незаконно размещают на своих страницах массивы персональных данных. Таким образом, на наш взгляд, термин «содержащий персональные данные» не позволяет блокировать корпоративные сайты (они, как правило, никаких незаконно размещенных данных не содержат), а также сайты, которые собирают персональные данные, но не публикуют их.

На наш взгляд, 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.

Петрусевич Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

АНАЛИЗ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Информация, составляющая коммерческую тайну, определяется как научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, в том числе ноу-хау, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьи лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности правовые, организационные, технические и иные меры охраны.

Согласно закону Российской Федерации от 21.07.1993 г. № 5485 – 1 (редакция от 08.03.2015 г.) «О государственной тайне» к коммерческой тайне относят также:

– знания и опыт в области реализации продукции и услуг, сведения о конъюнктуре рынка, результаты маркетинговых исследований;

– коммерческие, методические или организационно-управленческие идеи и решения.

Так же данный закон формулирует следующие положения:

– конфидент коммерческой тайны – физическое или юридическое лицо, которому в силу служебного положения, договора или на ином законном основании известна коммерческая тайна другого лица;

– режим коммерческой тайны – система правовых, организационных, технических и иных мер, принимаемых обладателем коммерческой тайны и конфидентом коммерческой тайны по обеспечению ограниченного доступа к соответствующей информации;

– носители коммерческой тайны – материальные объекты, в том числе физические поля, в которых информация, составляющая коммерческую тайну, находит отображение в виде символов, образов, сигналов, технических решений и процессов;

– разглашение коммерческой тайны – деяние (действие или бездействие), которое совершается с нарушением закона или договора (в том числе трудового) и в результате которого коммерческая тайна стала известна третьим лицам;

– неправомерные способы получения коммерческой тайны – собирание информации, составляющей коммерческую тайну, посредством похищения документов, подкупа или угроз, дачи взятки, введения в заблуждение, нарушения или подстрекательства (принуждения) к нарушению обязательств о соблюдении режима коммерческой тайны, а равно иным незаконным способом без согласия обладателя коммерческой тайны на передачу коммерческой тайны третьим лицам.

Нарушение прав на коммерческую тайну влечет за собой дисциплинарную, 'административную, гражданско-правовую, уголовную ответственность в соответствии с законодательством РФ.

Лицо, которому в силу трудовых отношений с обладателем коммерческой тайны – работодателем стала известна коммерческая тайна, в случае умышленного или неосторожного разглашения коммерческой тайны при отсутствии в действиях такого лица состава преступления несет дисциплинарную или гражданско-правовую ответственность в соответствии с законодательством РФ.

Органы государственной власти, иные государственные органы и органы местного самоуправления несут перед обладателем коммерческой тайны гражданско-правовую ответственность за разглашение или неправомерное использование коммерческой тайны должностными лицами таких органов, которым она стала известна в связи с выполнением ими служебных обязанностей.

Лицо, использовавшее коммерческую тайну и не имевшее достаточных оснований считать использование данной информации незаконным, в том числе получившее доступ к ней в результате случайности или ошибки, не может быть привлечено к ответственности. По требованию обладателя коммерческой тайны такое лицо обязано принять меры по ох ране коммерческой тайны. При отказе такого лица принять на себя обязательство о неразглашении коммерческой тайны обладатель коммерческой тайны вправе требовать в судебном порядке защиты своих прав.

Невыполнение законных требований должностных лиц органон государственной власти, иных государственных органов или органон местного самоуправления по доступу к коммерческой тайне, а равно воспрепятствование осуществлению этими должностными лицами возложенных на них служебных обязанностей влечет за собой административную ответственность в соответствии с законодательством РФ.

Таким образом, наше государство надежно защищает нас в области правового регулирования информационных отношений в области коммерческой тайны.

Солодовник В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время проблема борьбы с преступлениями в сфере высших технологий и информационной безопасности стоит крайне остро как перед правоохранительными органами Российской Федерации, так и перед правоохранительными органами всех стран мирового сообщества.

В Российской Федерации компьютерная преступность с каждым годом набирает обороты. Это происходит в связи со сложной криминогенной обстановкой в стране, отсутствием до недавнего времени уголовно-правовых механизмов воздействия на набирающую силу преступность в данной сфере. Также противодействие данной преступности требует от сотрудников правоохранительных органов специальных познаний в области компьютерных технологий, обеспечение их современной техникой и оборудованием. чтобы они могли активно противодействовать отдельным лицам и организованным группам, совершающим преступления в данной сфере.

Представляется необходимым разработать программу противодействия преступности в сфере информационной безопасности по следующим направлениям:

1. Развитие международного сотрудничества Российской Федерации в области обеспечения информационной безопасности. Данное сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности должны являться:

– недопущение и пресечение развития транснациональных преступных организованных групп, совершающих компьютерные преступления;

– обеспечение безопасности информационного обменана международном уровне, в том числе обеспечение сохранности информации при ее передаче по национальным сетям и каналам связи;

– предупреждение несанкционированного доступа к конфиденциальной информации, которая содержится в международных банковских сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области борьбы с организованными преступными формированиями, специализирующихся на совершении компьютерных преступлений. Эта деятельность должна включать в себя:

– создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;

– формирование нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в сфере компьютерной информации, а также порядок ликвидации последствий этих противоправных действий;

– разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;

– создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе

специализированных информационно-телекоммуникационных систем со свободным доступом правоохранительных органов различных государств.

2. обеспечение высокого уровня финансирования МВД России для улучшение материальной базы подразделений, занимающихся противодействием организованной преступности в том числе связанной с информационной безопасностью

3. Совершенствование сотрудничества и взаимодействия с иностранными спецслужбами в целях обмена информацией о преступлениях и преступниках в сфере информационной безопасности.

4. Обеспечение высокого уровня профессиональной квалификации сотрудников правоохранительных органов, привлечение специалистов из числа «молодых талантов» с предоставлением им соответствующего финансирования и материального содержания.

5. Организация научных исследований в области обеспечения информационной безопасности Российской Федерации, разработка специальных методик, позволяющих выявлять и привлекать к ответственности членов организованных преступных групп, занимающихся преступной деятельностью в сфере компьютерной информации.

В заключении следует отметить, что изложенные предложения по противодействию преступности в сфере компьютерной информации базируются, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Суровенко И.А., Быстрова Н.С.
Россия, Санкт-Петербург, РОПД ГСУ ГУ МВД России по Санкт-Петербургуи Ленинградской области

РОЛЬУГОЛОВНОГО КОДЕКСА В ОБЕСПЕЧЕНИИ ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время сформирована основная нормативная база по предупреждению и пресечению правонарушений в информационной сфере, которая предусматривает как гражданскую и административную, так и уголовную ответственность за совершение правонарушений и преступлений в информационной сфере. Вместе с тем с целью практического применения указанной нормативной базы существует немало трудностей, поскольку отсутствуют конкретные механизмы применения указанных норм на практике.

Основанием для возникновения юридической ответственности в сфере информационных отношений является юридический факт – совершение субъектом правонарушения в информационной сфере, то есть виновное, противоправное деяние (действие, бездействие) конкретного субъекта, посягающее на установленный информационный правопорядок и причиняющее вред информационной сфере, либо создающее реальную угрозу такого причинения. Несмотря на кажущую простоту, охрана данных общественных отношений, является важнейшим элементом в системе мер правового обеспечения информационной безопасности, защиты прав граждан, общества и государства в информационной сфере.

Действующее уголовное законодательство содержит группу норм, предусматривающих уголовную ответственность за информационные преступления. К таким категориямнорм, например, относят преступленияпротив конституционных прав и свобод человека и гражданина, имеющих информационный характер, категорию преступлений, затрагивающих вопросы информационной безопасности в сфере экономической деятельности. В целом же именно УК принадлежит особая роль в обеспечении правовой охраны информационной безопасности. В правоприменительной практике содержится ряд норм, специально предназначенных для защиты исследуемых отношений. Так, например, глава 28 “Преступления в сфере компьютерной информации” определяет, какие общественно опасные деяния в сфере компьютерной информации являются преступными.

Томашевич Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЗАЩИТА И БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКА

В настоящее время для получения, обработки, поиска и внедрения информации большой популярностью пользуется сеть Интернет. В связи с этим возрастает роль правовых механизмов, которые регулируют информационные отношения в обществе, включая в себя различные законодательства, предусматривающее, охрану авторского права, коммерческой и личной тайн, защиту потребителей от ложной информации, ответственность за пиратское распространение информации, защиту товарных знаков, знаков обслуживания.

Разберемся с понятием информационное правовое законодательство Российской Федерации: представляет собой совокупность норм права, регулирующих общественные отношения в

информационной сфере. В настоящее время законодательство формируется на основе разработки и принятия федеральных законов, а также законов субъектов Российской Федерации, которые регулируют отношения, касающиеся сферы информатизации - порядка создания, сбора, хранения, обработки и передачи информации.

Каждый человек, получая свою информацию из различных источник, может подвергнутся опасности, не защищая свои персональные данные. Чтобы получить информацию из сайтов, интернета зачастую людям необходимо вводить персональные данные например, имя, фамилию, номер телефона, дату рождения. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, которая включает в себя организационные меры и средства защиты информации (в том числе шифровальные (криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии». Методы и способы защиты информации в информационных системах устанавливаются ФСТЭК и ФСБ РФ в пределах их полномочий.

27 июля 2006 года приняли новый федеральный закон «О персональных данных» № 152 – ФЗ, который регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и доступ к таким персональным данным.

Цель федерального закона заключается в обеспечении защиты прав и свобод человека и гражданина при обработке его персональных данных, а также защиты прав на неприкосновенность частной жизни, личную и семейную тайну. В федеральном законе также раскрывается понятия о персональных данных – это любая информация, относящаяся к прямо или косвенно определенному физическому лицу. Уполномоченный орган по защите прав субъектов персональных данных имеет право: запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию; осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий; требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных; ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации; принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона.

Каждый человек вправе защищать и иметь доступ именно к своим данным, но не каждый человек сможет это сделать правильно без настоящего федерального закона. Лица, которые нарушают этот закон и его требования, несут предусмотренную законодательством Российской Федерации ответственность.

Харрасов Э.Э.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблема защита информации методами и способами права существует еще с 90-х годов. В первую очередь, интерес к противоправным действиям связанных с кражей информации касается государственных органов, энергетики, министерства обороны, сферы финансов, правоохранительной – несанкционированный доступ к которым может привести к серьезным последствиям. Так же, в настоящее время информация является серьезным оружием и компонентом неотъемлемой безопасности. Она может влиять мировые события, на политические отношения между странами, в зависимости от освещения информации она может влиять на умы народа, так же информация может способствовать развитию интеллектуального потенциала за счет использования интеллектуальной собственности и т.д.

Для надежности хранения информации необходимо обеспечить ее безопасность. Информационная безопасность Российской Федерации основывается на состоянии уровня

безопасности ее интересов в информационной сфере, устанавливающихся интересам личности, государства и общества.

К правовому регулированию безопасности информации в Российской Федерации относится создание нормативных правовых актов, устанавливающих правила и методы обращения с информацией, а так же создание рекомендаций по вопросам обеспечения информационной безопасности Российской Федерации.

Правовая защита информации включает в себя многочисленное число правовых актов, которые можно разделить на семь групп: Конституция РФ; общие законы, кодексы; законы об организации управления (нормы по защите информации); специальные законы, к которым относится и Закон РФ «Об информации, информационных технологиях и о защите информации»; законодательство субъектов Российской Федерации; подзаконные нормативные акты по защите информации; правоохранительное законодательство России (определяют ответственность за преступления и правонарушения в сфере информатизации).

Законодательство в области защиты информации может быть представлено множеством законов. Одним из важнейших в данной области является Закон «Об информации, информационных технологиях и о защите информации», который устанавливает базу правового определения наиболее значимых компонентов информационной деятельности.

Настоящий Федеральный закон регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Многообразие нормативно-правовых актов, касающихся обеспечения безопасности информации, разберем на группы по видам регламентируемых ими вопросов.

1. Права собственности, владения и распоряжения информацией. С этими понятиями связано понятие авторского права, которое нарушается посредствам «пиратства». Наибольшие потери от пиратской деятельности понесли в большинстве (более 2,8 млрд. долларов), Япония (больше 2 млрд. долларов) и Германия (больше 1,8 млрд. долларов). Впервые в России закон об авторском праве был принят в начале XIX века, затем указом Николая I срок защиты авторского права повысили до 50 лет. В 1995 г. Россия присоединилась к важным международным соглашениям в этой области – Бернской Конвенции и Римской Конвенции.

2. Степень открытости информации (правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб собственнику этой информации). Так, закон «Об информации, информационных технологиях и о защите информации» разделяет информацию на:

– документированная информация ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (ст.10, ч. 2);

– конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ст. 2).

Так же к категории конфиденциальной информации отнесены персональные данные о гражданах, (ст. 11, ч. 1).

Современное государство нуждается в создании нормативно-правовой базы обеспечивающей безопасность информации, а так же устранять угрозы и принимать меры против уже появившихся угроз. Безопасность информации становится все более важной, так как эффективность информационной безопасности в большой степени определяет место и роль государства в мировой политике. России необходимо пропагандировать свои культурные ценности и традиции в условиях развивающихся информационных технологий. Как и в любой другой сфере, здесь есть ряд проблем, которые требуют решения, к ним относится и пробелы в нормативно-правовых документах, а так же отсутствие достаточного числа специалистов по защите информации.

Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ТЕСТОВОГО КОНТРОЛЯ ЗНАНИЙ КУРСАНТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ОПЫТ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ)

Важной задачей в обучении является контроль знаний. Из всех рассмотренных форм организации контроля наиболее простой является форма тестирования. При проведении контроля она не требует творческого участия преподавателя в процессе, его функции сводятся к простому подсчету правильно указанных ответов. В силу указанных причин, возникла необходимость создания специализированного средства, позволяющего автоматизировать контроль знаний курсантов и слушателей. Авторский коллектив кафедр Санкт-Петербургского университета МВД России разработал программное средство «Компьютерная система тестирования», что позволяет рекомендовать ее для оценки текущих и остаточных знаний в любой предметной области.

Особенно важную роль разработанная система тестирования может играть при реализации модульного обучения, внедрение которого уже сейчас актуально при организации дистанционной подготовки и переподготовки сотрудников ОВД. Результаты входного и выходного тестового контроля позволят обучаемому правильно выбрать нужный модуль и построить процесс обучения в соответствии со своими способностями, наклонностями и задачами, которые поставили перед ним вышестоящие органы.

Средством разработки был выбран язык программирования Borland Delphi, который воплотил целый ряд передовых технологий в области разработки программных средств. В силу своей специфики данный язык программирования позволяет в кратчайшие сроки изменять, дополнять и совершенствовать программный продукт, а также использовать части кода в виде встраиваемых объектов в другие проекты.

Для разработки программы в рамках классической формы тестирования были сформулированы следующие требования:

– расширяемость, осуществляемая посредством независимых баз, содержащих вопросы, ответы, а также ключи к тестам;

– перемещение по списку вопросов;

– ответ на поставленный вопрос путем указания одного или нескольких правильных, по мнению обучаемого, вариантов;

– возможность пропуска вопроса, поставив правильность ответа на него под сомнение, что будет отражено на экране соответствующим образом.

При помощи организации тестирования на персональном компьютере предоставлена возможность реализовать следующие функции:

– учет собственного балла или веса вопроса в тесте;

– введение для каждого или всех вариантов ответов на вопрос шкалы степени уверенности в правильности выбранных альтернатив ответов;

– обеспечена нефиксированная последовательность подачи вопросов и ответов на них;

– наличие дополнительных вопросов по отношению к главному в иерархической последовательности;

– динамическое создание альтернатив ответов на вопрос.

– учет времени, затраченного на тестирование в целом или на ответ по определенному вопросу;

– автоматическое прекращение тестирование по истечению лимита времени;

– автоматизированное и единое применение различных критерий оценки результатов;

– просмотр результатов тестирования в виде таблицы и графика с последующим выводом на печать.

На сегодняшний день создана и активно применяется на кафедрах Санкт-Петербургского университета МВД России версия программы «Компьютерная система тестирования», в которой в полном объеме реализованы возможности классической формы тестирования, а также некоторые специфические функции, воплотившиеся в жизнь благодаря применению компьютера. Это такие функции как собственный бал или вес вопроса в тесте и введение для каждого из вариантов ответов на вопрос шкалы степени уверенности в правильности выбранных альтернатив ответов.

Первая специфическая функция позволяет дифференцировать вопросы внутри теста по своей принципиальной значимости. Так, например, неправильный ответ на принципиально значимый вопрос более отрицательно скажется на результате, чем неправильный ответ на принципиально менее значимый вопрос.

Вторая специфическая функция позволяет учесть эмоциональное состояние тестируемого относительно правильности своего ответа, что достигается путем указания степени его уверенности. Таким образом, неуверенный неправильный ответ менее отрицательно скажется на результате чем одновременно уверенный и неправильный ответ. В то же время, неуверенный правильный ответ даст меньший результат, чем мог бы дать уверенный правильный ответ. Данная специфическая функция позволит тестируемому сформировать определенную тактику поведения во время прохождения теста и будет развивать в нем качества, необходимые для умелого лавирования и рационального использования твердо усвоенных знаний.

Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕРМИНОЛОГИЯ

Информация в общем случае это сообщение. Передача сообщения оправдана только в том случае, если смысл, вкладываемый адресантом, без искажений воспринимается адресатом. При этом среди прочего необходимо обеспечить единый словарь, то есть понимание, вкладываемое в терминологию должно совпадать. Для этого употребляемые термины должны быть определены. Определение - это совокупность признаков, выделяющих объект из окружающей действительности.

К сожалению, на практике приходится сталкиваться с ситуацией, когда в термины вкладывается разное содержание, что влечет за собой возможность как нечеткого понимания сообщений, так и сознательное затуманивание смысла сообщений.

Иллюстрацией сказанного может служить термин "демократия". Широта его использования ни у кого, пожалуй, сомнений не вызовет. А вот когда речь заходит об определении, вряд ли возможно встретить два одинаковых. Более того, существуют разночтения даже относительно того, куда же демократия должна быть отнесена. Встречаются следующие области: разновидность режима; политический строй; организация; политическая система; форма правления; совокупность принципов и практических мер; форма государственно-политического устройства; механизм; образ государственного правления; политический строй; государственное устройство; народные массы; форма государственного устройства и т. д.

Таким образом, в настоящее время не существует общепринятого определения повсеместно используемого понятия "демократия". То же самое относится и к некоторым другим широко используемым терминам.Сложившаяся ситуация, с одной стороны, затрудняет понимание сказанного, а с другой - может быть использована для продвижения разрушительных интересов. Поэтому необходимо устранить этот пробел.

При этом необходимо исключить ситуацию, при которой единственным зарегистрированным в установленном порядке оказался орфоэпический словарь с более чем спорным произношением многих общеупотребительных терминов. Этот подход может быть обеспечен только путем широко обсуждения под эгидой уполномоченной государством организации.

Ярмоленко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России

СОСТОЯНИЕ И ВОЗМОЖНОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Интенсивное развитие информационно-коммуникационных технологий и широкое их применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры. Изменяя информационную среду общества, глобальная компьютерная информационная сеть Интернет и информационные технологии выступают в роли универсального метода информационно-психологического воздействия на личность и социальные коллективы. Электронные средства массовой информации как средства информационно-психологического воздействия на личность рассчитаны на убеждающее и на внушающее воздействие на личность.

Информатизация общества выдвигает определенные требования к информационно-психологической безопасности личности. Угрожая не только интеллектуальному, духовно-нравственному состоянию человека и его физическому здоровью, негативная информация воздействует на психологическое состояние личности. Источники информационно-психологической опасности для личности проявляются, прежде всего, через функционирование средств массовой коммуникации, действующих активно и целенаправленно разнообразных объединений или группировок граждан, а так же общественных, политических партий и движений, националистических, мафиозных организаций и религиозных сект, финансовых структур.

Вопреки желанию человека и его воли губительные информационные воздействия способны деструктивно изменять его психологические характеристики и поведение. Степень и формы технологий информационного давления зависит как от возраста личности, так и от его индивидуально-психических особенностей личности и, конечно, от жизненного опыта.

Информационно-психологическая безопасность личности понимается как определенное защищенность состояния психического сознания человека, реализуемое гражданские права и свободы в соответствии с нормами федерального законодательства и международного права.

Человек, обладающий знаниями и опытом, может создать психологический барьер обработки сознания информационными потоками, оперативно адаптируясь к меняющимся социальным условиям и к воздействиям как внешним, так и внутренним факторов. Средства и технологии манипуляции личностью относятся к внутренним факторам, к внешним факторам − средства и методы информационно-психологической агрессии со стороны участников информационного противоборства.

Формы, методы и технологии управления тайного принуждения личности используют в межличностном общении и массовой коммуникация. Однако все способы намеренной манипуляции личностью работают тогда и только тогда, когда они базируются на объективной базе, то есть существовании определенного мировоззрения личности, необходимого для определенного манипулирования.

Если же рассматривать понятие «безопасность» с психологической точки зрения, то оно раскрывается как защита психического состояния человека и его жизненных потребностей и

интересов для полноценного развития в обществе в социально-приемлемых формах. Объектами обеспечения информационно-психологической безопасности личности являются: сознание, система ценностей, психическое здоровье и свобода воли.

К источникам информационно-психологического воздействия на личность относят прежде всего государство (в том числе – иностранные государства), государственные структуры и учреждения, затем различные общественные, экономические, политические и иные организации, в том числе зарубежные, а так же различные социальные группы (формальные и неформальные) и устойчивые (либо случайные), большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и проведения досуга. К источникам угроз относят представителей государственных и общественных структур, разнообразных социальных групп.

Данная проблема может быть решена следующим образом:

– Применять способы нейтрализации негативных информационно-психологических воздействий.

– Развивать, укреплять и использовать адаптационные возможности личности к таким воздействиям.

– Создавать и применять методологию определенного морально-психологического климата в социуме, который бы способствовал противостоять информационно-психологическим воздействиям и успешно выполнять профессиональные задачи;

– Использовать формы и методы ликвидации или ослабления последствий нанесенного ущерба в условиях информационной глобализации общества.

Таким образом, невозможно обеспечить безопасность общества и государства, если не гарантирована информационно-психологическая безопасность личности.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена

РИСКИ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫКОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ НА ПЛАТФОРМЕ WINDOWS НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Широкое внедрение и использование компьютерных систем и технологий электронного обучения (КСИТЭО) в том числе на платформе WINDOWS направлено на повышение качества функционирования и обеспечение доступности научно-образовательной среды в Российской Федерации. Современные технологии КСИТЭО на платформе WINDOWS ориентируются на достаточно новые тенденции организации научного и учебного процесса: распределенные системы управления деятельностью и контентом, дистанционные технологии работы и учебы, персонализацию учета научных и образовательных достижений, генерацию индивидуальных образовательных маршрутов развития, разработку индивидуальных научных и учебных интерфейсов и программ, геймификацию форм и технологий творческого, научного и учебного процессов, интерактивность научно-исследовательских данных, форм обучения и учебного контента, разработку видеоигровых исследовательских моделей и учебных миров.

Эти тенденции позволяют в числе по-новому организовать международные процессы исследований или обучения - с возможностями оперативной актуализации новых данных или знаний на основе неформальных, но доступных личности каждого исследователя или обучаемого технологий доступа к информационным ресурсам. При этом местом осуществления научной или образовательной деятельности является место территориального нахождения научного или образовательного учреждения (НОУ) независимо от места нахождения исследователя или обучающихся. Для реализации новых форм и алгоритмов деятельности НОУ должны сформировать электронную информационно-образовательную среду, которая интегрирует информационно-образовательные ресурсы и сервисы, информационные, телекоммуникационные и технологические средства обучения, психологического сопровождения и контроля знаний учащихся на базе той или иной операционной системы или платформы функционирования КСИТЭО.

Однако в настоящее время на практике НОУ внедряющие и использующие КСИТЭО в основном работают на платформе WINDOWS и этой связи зачастую сталкиваются с множеством проблем, например отсутствия: 1) нормативно-правовых документов регулирующих режимы использования КСИТЭО, 2) лицензионных требований и аккредитационных показателей, регламентирующих деятельность КСИТЭО в НОУ, а также неурегулированостью вопросов авторских прав на электронные объекты интерактивной и гипертекстовой интеллектуальной собственности. Кроме того в новых условиях значительно увеличиваются риски несанкционированного доступа к персональным данным пользователей, использующих платформу WINDOWS, тем самым возникают новые информационные угрозы и потенциальные объекты рисков научно-образовательной и информационной безопасности вузов и школ РФ.

В статье предлагается оценить риски безопасного внедрения и использования моделей и технологий КСИТЭО использующих платформу WINDOWS которые ориентированы на: 1) технические ресурсы, глобальную сеть, сервисы, формы дистанционного и открытого образования, 2) научно-исследовательскую деятельность и разработку инновационных технологий, 3) сотрудничество с европейским сообществом в области науки, воспитания и образования в соответствии с европейскими ценностями и стандартами «открытого образования». С нашей точки зрения, например, научно-исследовательская и педагогическая методология российского сегмента КСИТЭО должна ориентироваться на национальные школы и традиции, философские учения и методы воспитания, в том числе на лучшие педагогические системы обучения школьников и студентов периода 50-80 х годов XX в., например, в области естественных и технических наук, активно воспитывая дух и идей патриотизма, дружбы народов исторически и географически связанных с Россией. Кроме того необходимо оценить возможные риски западного информационно-образовательного контента и так называемого «свободного» обучения в сети Интернет, а также потенциально возможные действия и угрозы глобальных провайдеров, расположенных например в США и Европе по возможному ограничению доступа российских НОУ и их субъектов к сервисам КСИТЭО, так как в случае

дальнейшей эскалации и обострения политических, экономических и социальных отношений в мире техническая и программная инфраструктура контента российского КСИТЭО использующих платформу WINDOWS, так или иначе, будет контролироваться зарубежными центрами и «исследовательскими» программами. Выделение классификации потенциальных угроз и рисков научно-образовательной среде со стороны КСИТЭО использующих платформу WINDOWS поможет НОУ принимать взвешенное решение о целесообразности развития КСИТЭО ориентированного на западные операционные системы, продукты, ресурсы, модели и сервисы интернет. Системы и технологии КСИТЭО использующие платформу WINDOWS как потенциальные объекты риска и информационные угрозы безопасности научно-образовательной среды Российской Федерации определяются возможными уязвимостями, выходами из строя, неправильной работой или нарушениями:

1. среды одновременного, отложенного, локального и глобального доступа, передачи, хранения или обработки научной, учебной, технической информации-контента;
2. в среде управления содержанием деятельности или документооборота,например в среде научных исследований, электронного обучения, а также несанкционированного доступа к персональным данным (информации) субъекта КСИТЭО;
3. бесперебойного функционирования серверов, коммуникационного оборудования в связи с отключением, выходом из строя или неправильной работой систем электропитания, блокированием и затруднением доступа в Интернет, блокированием доступа к сайтам и системам КСИТЭОна платформе WINDOWS;
4. уровней публичного и закрытого взаимодействия, секретности, целостности, доступности, штатной работы НОУ или субъектов КСИТЭОна платформе WINDOWS;
5. уровней физической и технической инфраструктуры НОУ или КСИТЭОна платформе WINDOWS;
6. уровней программного обеспечения КСИТЭОНОУ или субъекта КСИТЭОна платформе WINDOWS;
7. уровней кадровых ресурсов функционирования КСИТЭОна платформе WINDOWS НОУ или дефицита компетенций научных сотрудников, преподавателей или обучаемых;
8. нормативно-юридических уровней обеспечения работы КСИТЭОна платформе WINDOWS;
9. организации научно-методической деятельностиКСИТЭОна платформе WINDOWS;
10. организационно-административной деятельности КСИТЭОна платформе WINDOWS;
11. организации научной и психолого-педагогической поддержки субъектов КСИТЭОна платформе WINDOWS,
12. медико-биологического и экологического состояния инфраструктуры организаций использующихКСИТЭОна платформе WINDOWS;
13. финансово-экономических ресурсов организаций, научных и образовательных сообществ, а также возможностей сотрудника или обучаемого на основе КСИТЭОна платформе WINDOWS;
14. в среде и инфраструктуре социальных, политических и государственных образованийроссийского общества, в том числе непосредственно внедряющих и поддерживающих технологии КСИТЭОна платформе WINDOWS.

Агеева Е.С., Прохоров А.И., Смагулова А.С., Золотарев В.В.
Россия, Красноярск, Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнёва

РАЗРАБОТКА МЕТРИЧЕСКОГО СПОСОБА КЛАССИФИКАЦИИ ПРОГРАММНОГО КОДА

Многие алгоритмы поиска вредоносного программного кода производят поиск, основываясь на сигнатурах. Данный метод состоит в том, что система поиска обращается к словарю с известными вредоносными программными обеспечениями, или вирусами, составленному разработчиком системы. Если находится соответствие какого-либо участка кода просматриваемой программы известному коду, или сигнатуре, вредоносного кода в словаре, то система поиска производит предусмотренные для этого действия. Такой метод имеет некоторые недостатки, связанные с тем, что словарь следует периодически обновлять, а так же при появлении нового, еще неизвестного вредоносного программного кода, система может не выявить угрозы.

Для устранения недостатков, перечисленных выше, предлагается использовать эвристический алгоритм поиска вредоносного кода. В качестве такого алгоритма представлен метрический способ классификации. Идея этого способа заключается в том, что существует зависимость собранных метрик программного кода от типа этого кода: вредоносный программный код или легитимная программа.

Проверка, представленной выше, идеи осуществлялась с помощью скрипта IDAMetrics, программы IDA 5.5.0, IDApython 1.2.0 и Python 2.5. С помощью установки данных компонентов была настроена рабочая среда. Скрипт IDAMetrics, который для автоматизации работы был модифицирован, выполнял функцию по сбору метрик с программного кода вирусов и легитимных

программ. Под метриками понимается мера, позволяющая получить численное значение некоторого свойства программного обеспечения или его спецификаций. Использовались такие группы метрик, как количественные, метрики сложности потока управления программы, метрики сложности потока данных программы и гибридные метрики. Каждая группа метрик и каждая метрика оценивает какое-либо свойство программного кода, поэтому перед реализацией какой либо метрики следует изучить, на что она направлена, и будет ли она полезна.

После завершения скрипта по сбору метрик были получены две папки с текстовыми файлами: для вредоносного программного кода и для легитимных программ. Каждый текстовый файл содержит в себе общее количество значений метрик и значения метрики по каждой функции программного кода. Для оценки зависимости значения метрик от типа программного кода были представлены три способа представления полученных данных. Было предположено, что при оценке зависимости с помощью графиков, возможно будет проанализировать и визуально или аналитически построить поверхность разделения на базе одной из метрик (критериев), которая служила бы границей между легитимными программами и вредоносным программным кодом.

Для первого способа использовались только метрики программного кода. Было построено 171 графика с результатами зависимости каждой метрики от каждой. При просмотре графиков было выяснено, что данный способ не может быть применен в качестве оценки, так как нельзя было провести условную разделяющую линию (поверхность разделения).

Во втором способе использовались как метрики программного кода, так и размер файлов в байтах. Было построено 19 графиков зависимости значения каждой метрики программного кода от его размера. По результатам был сделан вывод, что данный способ также нельзя использовать.

Третий способ помимо метрик программного кода, его размера, включал еще и количество функций в программном коде. Графики были построены в трехмерном виде, где отображалась зависимость метрики, размера программного кода и количества функций друг от друга. Такой способ оказался наиболее информативным. Метод нуждается в совершенствовании, поскольку на текущем этапе такая эвристика показывает низкие результаты по проценту ошибок второго рода, а также очень чувствительна к некоторым способам обработки программного кода (к примеру, обфускации).

Для того чтобы метрический способ классификации программного кода был применим, следует решить задачи, связанные с распаковкой и деобфускацией программного кода. Так как при помощи запаковки и обфускации вредоносного программного кода, его невозможно в некоторых случаях отличить от легитимной программы. Для решения таких задач следует применить машинное обучение.

По итогу решения выдвинутых задач, метрический способ классификации программного кода можно будет применять в различных системах обнаружения вирусов и в анализаторе трафика для выявления вредоносного программного обеспечения, что значительно повысит информационную безопасность компьютерных систем.

Работа выполнена в рамках гранта Президента молодым российским ученым - кандидатам наук, договор №14.Z56.15.6012 от 16.02.2015 г.

Александров В.А., Десницкий В.А., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»

РАЗРАБОТКА И АНАЛИЗ ФРАГМЕНТА ЗАЩИЩЕННОЙ СИСТЕМЫ, РЕАЛИЗУЮЩЕЙ КОНЦЕПЦИЮ ИНТЕРНЕТ ВЕЩЕЙ

В работе исследуются вопросы разработки и реализации систем, использующих концепцию Интернет вещей. Под Интернетом вещей понимают систему аппаратных устройств специализированного назначения, в которые встраиваются электронные модули для управления ими и организации коммуникаций. В работе определяются актуальные угрозы и необходимые защитные меры, необходимые в процессе разработки фрагмента программно-аппаратной системы Умный дом в части осуществления контроля доступа в помещение с использованием языка Python и одноплатного компьютера Raspberry Pi (RPi). Приводится пример реализации одной из актуальных угроз, а также представлена реализация защитных мер от выбранной угрозы.

В целях обеспечения безопасности и выбора защитных мер в рамках разработанного фрагмента Умного дома применяется детальный анализ рисков. Данный анализ включает идентификацию активов, оценку возможных угроз, которым могут быть подвержены активы, а также относительную оценку уровня их уязвимости. По результатам этих операций выполняется оценка рисков и последующее определение обоснованных защитных мер. Анализ рисков проводится при помощи идентификации нежелательных событий и определения вероятности их появления. Нежелательные события могут влиять на корректность работы системы или ее пользователей. Такое неблагоприятное воздействие нежелательных событий является сложным сочетанием возможных видов ущерба, наносимого стоимости активов, подвергающихся риску. Вероятность такого события

зависит от ценности актива для потенциального нарушителя, вероятности реализации угроз и уровня доступности методов для использования уязвимых мест системы.

Методологически проведенная работа включает выполнение следующих действий: описание этапов обеспечения безопасности разрабатываемой системы; определение ограничений, применяемых в процессе анализа, в том числе ограничений на учитываемые активы и ресурсы; оценку угроз информационной безопасности; идентификацию существующих защитных мер и обоснованный выбор необходимых защитных мер. В процессе практической реализации устройство одноплатный компьютер Raspberry Pi используется как центральное управляющее устройство, так как это небольшое по размерам и недорогое типовое программно-аппаратное устройство. Небольшие размеры обеспечивают широкие возможности по его встраиванию в элементы существующей аппаратно-технической инфраструктуры. Аппаратные возможности этого устройства позволяют производить управление всей программно-аппаратной системой Умного дома. Наличие стандартизированных пинов GPIO позволяет подключать к RPi различные датчики и другие периферийные устройства. К RPi подключается светодиод, который загорается в случае несанкционированного проникновения в помещение Умного дома. Наличие операционной системы Linux позволяет осуществлять программирование системы Умного дома на нескольких языках программирования, поддерживающих эту операционную систему.

В качестве результатов проведенного анализа разработанной систем обосновывается получение следующих рекомендаций, направленных на повышение защищенности целевой системы. К защитным мерам необходимо отнести периодическую проверку работоспособности всех элементов системы. Это требуется в целях уменьшения вероятности аппаратных сбоев. Исходя из существующих защитных мер, на предприятии должна быть организованна защищенная корпоративная сеть. Это уменьшит вероятность перегрузки трафика, нарушения конфиденциальности, целости, доступности информации, передаваемой или обрабатываемой в рамках программно-аппаратной системы. Также во избежание нарушения целостности передаваемой информации, передаваемой между клиентом и сервером необходимо применять шифрование и хеширование. Для уменьшения вероятности использования программного обеспечения несанкционированными пользователями или несанкционированным способом необходимо устранить все критичные уязвимости используемых библиотек, приложений и операционной системы. Должно быть реализовано разграничение прав доступа, не позволяющее непривилегированным пользователям вносить какие-либо критически важные изменения, а также получать внутреннюю информацию системы. Также лишь администратор должен иметь права для установки программного обеспечения в центр управления, чтобы понизить риски установки вредоносного программного обеспечения. Для уменьшения вероятности использование программного обеспечения несанкционированными пользователями необходимо передавать и хранить пару <логин, пароль> в виде результата хеш-функции.

Работа выполняется при финансовой поддержке государственного контракта №14.604.21.0033 (уникальный идентификатор соглашения RFMEFI60414X0033).

БарышниковаН.Ю., ЕгоровА.Н., КрупенинаН.В., ТындыкарьЛ.Н.
Россия,Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ЭЛЕКТРОННОГО ТЕСТИРОВАНИЯ ДЛЯ ОЦЕНКИ СООТВЕТСТВИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ РАБОТНИКОВ МОРСКИХ СПЕЦИАЛЬНОСТЕЙ

Подготовка новых высококвалифицированных специалистов, а также организация мероприятий по повышению квалификации и переподготовке уже имеющихся кадров в области морских специальностей является актуальной в течение уже многих лет. Одним из возможных вариантов упрощения решения данной задачи является разработка специализированных тестов для оценки соответствия профессиональных компетенций работников морских специальностей.

В настоящее время для решения кадрового вопроса активно внедряются и используются информационные технологии, предоставляющие новые возможности по проведению электронного тестирования для объективной оценки знаний. Как правило, офисы фирм территориально удалены друг от друга, поэтому требуется организация единого программного комплекса для совместной работы. В этих условиях актуальной становится задача создания распределенной системы подготовки и проведения тестирования.

При работе распределенной информационной системы остро встают вопросы организации информационной безопасности ее функционирования, поскольку информационная база [ИБ] может содержать как персональные данные пользователей, так и закрытую профессиональную информацию в рамках содержания тестов.

Основная информационная система современного предприятия должна удовлетворять как минимум, следующим требованиям безопасности: достаточно низкая вероятность сбоя системы по

внутренним причинам, надёжная авторизация пользователей и защита данных от некорректных действий, эффективная система назначения прав пользователей, оперативная система резервного копирования и восстановления в случае сбоя.

Этим условиям в значительной степени отвечает среда 1С:Предприятие 8, в которой реализован программный комплекс организации тестирования, поддерживающий работу пользователя через удаленное интернет-соединение с помощью веб-браузера посредством механизма управляемых форм. Наличие удаленного доступа позволяет реализовать кросс-платформенность и независимость пользовательской среды от внешних факторов.

В качестве связующего звена интернет-соединения был выбран сервис «1С:Линк», который позволяет пользователям прикладных решений фирмы «1С» самостоятельно организовать безопасный доступ через Интернет к приложениям «1С» в офисе или дома – информационные базы хранятся на компьютерах фирмы в головном офисе.

Особое внимание сервиса уделено вопросам безопасности передаваемых данных. 1С:Линк обеспечивает шифрованный канал доступа (туннель), с помощью которого осуществляется быстрое и безопасное подключение к опубликованным на локальном веб-сервере файловым и серверным информационным базам приложений. Обмен зашифрованными данными происходит по протоколу TSL – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет. При этом используется ассиметричная криптография для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Благодаря протоколу TSL предотвращается прослушивание и несанкционированный доступ к информации. Стоит отметить, что все передаваемые данные также зашифрованы индивидуальным ключом, который хранится только на стороне пользователя.

Для работы через 1С:Линк не требуется внешнего IP-адреса. При этом рабочий компьютер пользователя становится «невидимым» в сети Интернет, что исключает возможные хакерские атаки. Также для доступа к информационным базам, хранящихся на серверах фирмы «1С», предусмотрена дополнительная процедура авторизации.

Сервис функционирует по принципу туннелирования сетевого трафика. Связь «точка-точка» обеспечивает передачу исключительно веб-трафика по протоколу HTTPS, а не сетевую маршрутизацию, защищая компьютер от потенциальных сетевых угроз.

Дополнительным источником защиты передаваемой информации также служит использование индивидуальных доверительных SSL сертификатов, предоставляемых каждому абоненту сервиса, которые подтверждают гарантированный уровень безопасности установленного подключения.

Информационная база тестовой системы работает в клиент-серверном режиме, при котором пользователи не имеют прямого непосредственного доступа к ней. «Посредником» между клиентами 1С:Предприятия 8.1 и сервером СУБД является рабочий процесс «rphost», который обращается с запросом к СУБД от имени своей учетной записи и затем полученный результат возвращает клиенту..

Созданная распределенная информационная система подготовки и проведения электронного тестирования для оценки знаний и умений специалистов в морской области в полной мере обеспечивает надежное хранение и безопасную передачу данных.

Бачурин И.В., Касаткин В.В., Лысенко В.А., Кузнецов А.Ю., Чендрова Ю.В., Сальникова П.Ю., Сычугов Д.С.
Россия, Архангельск, Агентство записи актов гражданского состояния Архангельской области Санкт-Петербург, Объединенный учебно-методический совет по направлению «Информационные системы и технологии», Санкт-Петербургский государственный университет технологии и дизайна, ООО «Ультраполимеры», ЗАО «ЛюксофтПрофешонал» Ростов-на-Дону, Ростовский государственный университет путей сообщения

БЕЗОПАСНОЕWEB-ПРИЛОЖЕНИЕДЛЯ УПРАВЛЕНИЯ ИМУЩЕСТВЕННЫМ КОМПЛЕКСОМ УНИВЕРСИТЕТА

Опыт внедрения и эксплуатации программного комплекса «Имущество университетов», разработанного на платформе IBM Notes/Domino [Верескун В.Д, Касаткин В.В., Лысенко В.А. и др. Опыт внедрения и использования информационно-аналитической системы поддержки принятия решений и управления имущественным комплексом Ростовского государственного университета путей сообщения. Региональная информатика (РИ-2014). XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции. \ СПОИСУ. – СПб, 2014. – 637 с. С. 223], продемонстрировал возможность повышения эффективности и качества управления имущественным комплексом государственных университетов, что играет важную роль при оценке эффективности их деятельности.

Анализ особенностей функционирования программного комплекса в ряде университетов Российской Федерациипоказал необходимость разработки соответствующего Web-приложения, внедрение которого при наличии большого количества пользователей позволяет существенно снизить затраты на приобретение и адаптацию комплекса. При этом особе внимание должно быть уделено

вопросам обеспечения информационной безопасности работы с приложением, оперирующим с данными, критически важными для организации.

При создании Web-версии программного комплекса использована технология IBMXPages, которая является составной частью программного обеспечения приложений на платформе IBM Notes/Domino, представляющей собойдокументо-ориентированную СУБД с архитектурой «клиент-сервер». Для разработки приложений на основе XPages использовано программное обеспечение IBM DominoDesigner. Создание графического интерфейса пользователя по технологии XPagesпроведено на основе стандартовWeb-разработки HTML, CSS и JavaScript.Web-приложение развернуто на сервереDomino с применением стандартного инструментаIBM DominoAdministrator.

Тестирование показало, что созданное с помощью XPages приложение является кроссплатформенным решением и доступно из таких Web-браузеров как InternetExplorer, GoogleChrome,Яндекс.Браузер, Opera, в т.ч. с мобильных устройств, функционирующих под управление ОС Android 5.0 и iOS 8.2.

Требования по защите информации при обработке конфиденциальных данных, предъявляемые к Web-приложению, могут быть реализованы на платформе IBM Notes/Domino на основе применения криптофункций шифрования и электронной цифровой подписи с использованием открытых ключей, являющихся базовыми сервисами ядра IBM Notes. Каждый пользователь при регистрации получает пару ключей: открытый ключ хранится в общей (публичной) адресной книге и доступен пользователям для считывания с сервера, а секретный ключ хранится в идентификационном файле пользователя локально.Электронная цифровая подписьиспользуется: при аутентификации сервером пользователя, при определении уровня доверия выполняемому коду, при проверке достоверности документов в базах данных и отдельных полей.Шифрование применяется для всех баз данных, входящих в состав программного комплекса «Имущество университетов», а также отдельных документов в базах данных, отдельных полей и информационного трафика.

Таким образом, разработанное Web-приложение программного комплекса «Имущество университетов» обладает необходимой степенью защищенности и может успешно использоваться на стационарных и мобильных платформах.

Бачурин И.В., Лысенко В.А., Чендрова Ю.В., Кузнецов А.Ю., Сычугов Д.С., Сальникова П.Ю.
Россия, Архангельск, Агентство записи актов гражданского состояния Архангельской области
Санкт-Петербург, Санкт-Петербургский государственный университет технологии и дизайна», ЗАО «Люксофт Профешонал», ООО «Ультраполимеры»
Ростов-на-Дону, Ростовский государственный университет путей сообщения

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ПЛАТФОРМЕ IBM NOTES/DOMINO

Платформа IBMNotes/Domino предоставляет широкие возможности по реализации информационной безопасности информационных систем различного уровня защищенности.

Сервер Domino обеспечивает свои приложения многослойной системой безопасности:

– Network (сеть) - данный уровень относится к возможности доступа к серверу по сети (физической возможности);

– Authentication (аутентификация) - процесс установления "доверия" между сервером и тем, кто пытается обращаться к серверу;

– Domino Server Security (безопасность на уровне сервера Domino) - данный уровень относится к ограничениям, определяемым в серверном документе Server;

– Database Access (ACL) (список управления доступом БД) - данный уровень относится к ограничениям, определяемым в списке управления доступом конкретной базе данных. Определяется независимо для каждой базы Lotus Domino и представляет семь настраиваемых основных уровней доступа;

– Design Element Security (безопасность на уровне элементов дизайна) - данный уровень относится к ограничениям, определяемым в списке управления данного элемента дизайна (т.е. кто может работать с этим элементом дизайна);

– Document Security (безопасность на уровне документа) - данный уровень относится к ограничениям, определяемым в полях типа Readers и Authors;

– Field Security (безопасность на уровне полей) - данный уровень относится к шифрованию информации из полей с включенным свойством поддержки шифрования (Enable encryption).

Также платформа предоставляет следующие возможности:

– настраиваемые политики паролей - эта функциональность позволяет администраторам наложить на пароли требования, соответствующие практически любым запросам, которые налагает система безопасности корпорации или государственной организации;

– поддержка более длинных ключей - по мере того как растут вычислительные мощности, растет и необходимость увеличивать длину ключей, чтобы защититься от взлома методом подбора;

– настройка сроков действия паролей и сертификатов - возможность настраивать срок действия паролей и сертификатов;

– улучшения, связанные с проверкой общих ключей – возможность применять дополнительный уровень проверки общих ключей (public keys) путем сравнения значения ключа, передаваемого в сертификате, со значением ключа, указанного в Domino Directory.;

– улучшения, связанные с восстановлением ID - для каждого администратора пользовательский ID-файл содержит пароль восстановления, который генерируется на случайной основе и шифруется общим ключом администратора. Этот пароль уникален для каждого администратора и для каждого пользователя;

– единый вход в систему (single sign-on) и соответствия имен (name mapping) в Domino - Cookie или маркер LTPA, который создается в ходе аутентификации пользователей при единой регистрации (single sign-on, SSO), включает в себя имя прошедшего аутентификацию пользователя. Когда система Domino создает маркер LTPA, она по умолчанию помещает уникальное имя в маркер LTPA.

В докладе рассмотрены примеры обеспечения информационной безопасности различных приложений на платформе IBM Lotus Notes/Domino.

Проведен анализ решений IBM Connections Family с использованием Vantage for IBM Connections, обеспечивающим безопасность, управление и контроль соответствия требованиям IBM Connections.

Особое внимание уделено анализу информационной безопасности специально разрабатываемых на платформе IBM Lotus Notes/Domino баз данных с удаленным распределенным доступом, в том числе с использованием web-интерфейса и мобильных платформ.

Таким образом, платформа IBM Lotus Notes/Domino позволяет создавать приложения с высоким уровнем информационной безопасности.

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

УСТРАНЕНИЕ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В МОДУЛЕ ФОРМИРОВАНИЯ СТРУКТУР ДАННЫХ ПРИ ПРОВЕДЕНИИ ИССЛЕДОВАНИЯ

В связи с проведением различных статистических исследований возникает необходимость получения достоверной информации для её дальнейшего анализа и прогнозирования тенденций в рамках исследуемой области. Подготовка к выполнению сбора разнородных статистических данных является трудоемким процессом, что приводит к возникновению ошибок и снижению эффективности работы персонала.

Разработан программный модуль, реализующий удобный пользовательский интерфейс и функционал для формирования структур данных будущих отчетов различной степени сложности. Улучшение, в основном, направлено на повышение удобства использования программного комплекса, на снижение требований к квалификации обслуживающего комплекс персонала (отсутствие необходимости специальных знаний в области программирования, специализированных языков конструирования запросов к базам данных и т.д.), и на максимально возможное устранение влияния человеческого фактора на результаты обработки собранных данных. Программный модуль формирования структур данных позволяет вести эффективную разработку структуры собираемой информации, автоматически организовывать каталоги для дальнейшего хранения и обработки собранных данных, дает пользователю возможность редактировать ранее созданные проекты при возникновении необходимости, обеспечивает упорядоченность и структурированность базы данных, существенно сокращает временные затраты оператора.

Модуль обеспечивает визуализацию результатов задач анкетирования с учетом внесения изменений в содержание анкет, при которых должна изменяться и структура объектов, заложенных в базе данных. Поскольку внесение изменений в типовом решении предполагает наличие специальных знаний в области баз данных и программного обеспечения, необходим высококвалифицированный специалист. В предложенном конструкторском решении данный процесс решается программными средствами автоматизации.

Разработанный программный модуль в составе применяемой системы использует реляционную базу данных, в которой данные представляют собой набор отношений. В качестве системы управления базами данных используется Microsoft Access – функционально полная реляционная СУБД, доступ к данным которой из программного кода осуществляется при помощи ее родного драйвера Microsoft Jet OLEDB 4.0.

Поскольку программный комплекс рассчитан на длительный период использования, работу с модулем создания структуры таблиц было решено организовать в виде проектов. Каждый из проектов сохраняется в базе данных, которая содержит две группы отношений: системная часть, обеспечивающая полноту и точность данных для описания и управления объектами программных

модулей, и часть с результатами анкетирования. Вторая часть представляет собой набор метаотношений, содержащих поля, сгруппированные тематически при создании структуры проектов. База позволяет беспроблемно эксплуатировать систему и выполнять ее текущее обслуживание.

При проектировании программного продукта был выдвинут ряд функциональных требований, позволяющих в полной мере реализовать идею быстрого создания безошибочной структуры данных неквалифицированным человеком. Взаимодействие пользователя со сложной логикой, заложенной в коде, осуществляется через небольшой набор визуальных компонентов – форм, каждая из которых выполняет свое особое предназначение. Программный модуль реализован на языке Object Pascal в среде разработки Borland Delphi.

Выбранные конструкторские и программные решения позволяют максимально сократить участие человека в составлении отчетов, анкетировании, группировании результатов анкетирования в разрезе различных аналитических критериев, тем самым заметно снизить или устранить искажающее влияние человеческого фактора в модуле составления отчетов и формирования структур данных для отчета.

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

МЕТОДЫ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ

В современном мире зависимость общества от компьютерных технологий увеличивается с каждым годом. Компьютерные сети охватывают все большую часть человеческой сферы деятельности и требуют обеспечения безопасности передаваемых по них конфиденциальных данных. Важной задачей является обнаружение сетевых аномалий и предотвращение попыток несанкционированного доступа к критическим данным.

Для обнаружения и классификации сетевых атак в большинстве случаев на практике применяется сигнатурный подход, который заключается в выявлении аномального поведения пользователя или системы согласно заданным шаблонам или правилам. Одним из очевидных недостатков этого метода является ориентация подобных систем на определенные типы атак и фиксированные шаблоны их обнаружения. Разработка адаптивных методов распознавания атак является актуальным направлением при решении задач обнаружения и классификации аномалий в сетевом трафике. В первую очередь это связано с непостоянством природы сетевого трафика и наличием статистических всплесков, свойственных как для легитимной, так и для аномальной сетевой активности. Применение эвристических средств анализа данных позволяет выявлять аномальные отклонения и строить правила для их обнаружения на основе имеющихся зависимостей объектов от их меток.

Процесс обнаружения и классификации образцов сетевых соединений состоит из нескольких фаз. Сначала осуществляется перехват пакетов, поступающих на один или несколько интерфейсов сетевой карты. Поток передаваемых данных формируется в сетевые соединения (набор IP-пакетов, передаваемых между парой хостов) и преобразуется в вектор параметров, характеризующих это соединение. Классифицируемый объект, представляющий собой список вещественных атрибутов каждого отдельного соединения, подается на вход обученных классификаторов для определения класса объекта.

Алгоритм формирования обучающего и тестового множеств можно описать следующим образом. На вход системе подается маркированный поток сетевых данных или бинарный файл с описанием классов атак, который представляет собой дамп сетевого трафика за определенный интервал времени. По мере его просмотра система формирует параметры, необходимые для классификации сетевых аномалий. Атрибуты трафика извлекаются из пакетных заголовков, включают количественные данные, характеризующие сетевые соединения, и содержат статистические показатели относительно открытых соединений на наблюдаемом хосте, собранных к моменту обработки данной сессии. После этого происходит добавление сформированных записей в обучающее или тестовое множество. Для обучения классификаторов применяются техники стандартного и каскадного обучения. Сперва настраиваются весовые коэффициенты базовых классификаторов на предварительно сформированных данных, затем обучаются верхнеуровневые классификаторы на выходных данных нижележащих классификаторов.

В качестве базовых бинарных классификаторов были выбраны нейронные сети, иммунные системы, нейронечеткие классификаторы и классификаторы на основе метода опорных векторов. Выбранные детекторы были объединены в итоговый классификатор, который принимал окончательное решение о соотнесении входного объекта к одному из возможных классов. Для проведения экспериментов было использовано несколько схем комбинирования, а именно решатель с использованием голосования по большинству, арбитр на основе областей компетентности и классификационное бинарное дерево. Результаты экспериментов показали, что наиболее

эффективной оказалась схема объединения детекторов в классификационное дерево с узлами, которые представлены нейронными сетями. Анализ проведенных экспериментов показал, что композиции базовых классификаторов имеют более высокие показатели распознавания атак по сравнению с отдельно взятыми классификаторами.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451) и программы фундаментальных исследований ОНИТ РАН (контракт №1.5).

Бурлов В.Г., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТУРЕ УПРАВЛЕНИЯ ВЫСШИМ УЧЕБНЫМ ЗАВЕДЕНИЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АНАЛИТИЧЕСКО-ДИНАМИЧЕСКОЙ МОДЕЛИ

В настоящее время ускорилось движение во всех сферах жизни общества. Повысился спрос на квалифицированные кадры выпускаемые из высших учебных заведений (ВУЗов). Повышения качества образования зависит от многих факторов в том числе и от принятия управленческих решений принимаемых руководителем ВУЗа.

Управленческое решение это свойство деятельности человека, которое позволяет обеспечить субъектом условия реализации предназначения объекта управления в соответствующей обстановке.Обстановка подразумевает собой совокупность факторов и условий, в которых осуществляется деятельность ВУЗа.

Ведется постоянная информационно-аналитическая работа по непрерывному сбору, изучению, анализу и отображению данных об обстановке, такие как разведка, мониторинг, маркетинг.

Для быстрого и своевременного реагирования на возникающие информационные угрозы, каждый руководитель должен задействовать ресурсы власти в рамках правовых норм. Ресурсы власти - все те средства, использование которых обеспечивает влияние на объект в соответствии с целями субъекта в соответствии с нормативно-правовыми документами.

Любое управленческое решение в том числе и управленческое решение руководителя ВУЗа принимается на основе модели. Модель – это описание или представление объекта, соответствующего данному объекту и позволяющая получать характеристики об этом объекте.

Управленческое решение представляет собой процесс распознания или идентификации проблемы и выработки команды по задействованию ресурсов позволяющих решать возникающие проблемы, то есть каждая проблема, возникающая перед руководителем ВУЗа, распознаётся и нейтрализуется.

В современных условиях, в частности при участии Web технологий широкие возможности для реализации процесса управления открывает использование сайта учебного заведения.В связи с этим особо актуальным ставится вопрос о разработки формализованной модели, которая позволяет с одной стороны передать суть управленческого решения, а с другой стороны использовать сайт учебного заведения в интересах повышения эффективности управления ВУЗом в условиях различных информационных угроз и не всегда корректных юридических оснований для реализации такой деятельности (правовые вопросы, персональные данные, закрытая информация).

Работа посвящается согласованию противоречивых факторов в интересах обеспечения требуемых показателей эффективности реализации управленческого решения руководителем ВУЗа. На основе использования правовой базы, программно-аппаратного комплекса и метода математического моделирования.Результаты данной работы позволяют формировать процессы гарантированного управления ВУЗом на основе использования сайта в условиях обеспечения информационной безопасности и правовых аспектов. Эта работа позволяет решать, что каждая возникающая в системе угроза будет распознана и устранена в рамках ресурса власти, которым располагает руководитель ВУЗа.

БушуевС.Н., Чечулин А.А., Проноза А.А.
Россия, Санкт-Петербург, ЗАО «НПП «ТЕЛДА», Санкт-Петербургский институт информатики и автоматизации Российской академии наук

КЛАССИФИКАЦИЯ ИСТОЧНИКОВ ДАННЫХ О СЕТЕВЫХ ОБЪЕКТАХ И СВЯЗЯХ МЕЖДУ НИМИ

Системы управления событиями и информацией безопасности (SIEM) предполагают оперативный сбор, хранение, обработку и последующую визуализацию данных о событиях, связанных с безопасностью. Изначально эти данные формируются и фиксируются в системных журналах различных аппаратных и программных элементов компьютерной инфраструктуры, образуя тем самым многомерные данные разнородной структуры.

Источниками информации об сетевых объектах могут выступать различные программные и программно-аппаратные комплексы мониторинга безопасности, системы оценки защищенности сети, средства анализа сети, коммутационное оборудование, рабочие станции пользователей, открытые телекоммуникационные сети и иные узлы компьютерной сети, содержащие сведения, необходимые

для осуществления мониторинга и управления информационной безопасностью информационно-телекоммуникационных систем.При наличии множества источников информации об информационных объектах возникает необходимость классификации этих источников с целью унификации последующих механизмов извлечения информации.

Все источники данных следует разделить на два класса – физические и логические.

Под физическим источником информации в общем случае будем понимать произвольный узел сети N, в том числе и внешний по отношению к этой сети, на котором установлено программное обеспечение, способное отслеживать и протоколировать события безопасности.

По отношению к сети физические источники информации следует условно разделить на внутренние и внешние.

К внутренним источникам относятся узлы самой сети. По характеру получаемых данных, внутренние источники подразделяются на сетевые и хостовые. Сетевые источники собирают данные о работе всей сети или конкретного ее сегмента. К таким источникам относят, например, сканер сети на наличие уязвимостей, сетевой экран, анализатор сетевого трафика, сборщик данных о сетевой архитектуре и доступности ресурсов. Хостовые источники собирают информацию о хосте, на котором они установлены. Примерами хостовых источников информации может быть антивирусное средство или иное программное обеспечение, установленное на хосте, такое как база данных, сервер удаленного доступа.

Внешним по отношению к сети источником может быть глобальная сеть Интернет, содержащая сигнатуры атак, антивирусные базы и иные формализованные сведения по компьютерной безопасности. Одним из внешних источников данных являются также существующие открытые базы данных, например, базы данных описания уязвимостей.

К логическим источникам информации относятся компоненты системы оценки защищенности сетевых объектов. Примерами логических источников информации могут быть узлы сети, способные вычислять количественные показатели безопасности информационных объектов, такие как уровень критичности, степень уязвимости, вероятность успешной атаки, стоимость обрабатываемой информации.

РаботавыполненаприфинансовойподдержкеМинистерства образования и науки Российской Федерации (контракт № 14.604.21.0137, уникальный идентификаторRFMEFI60414X0137).

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

ПРОЦЕССИНГОВЫЙ ЦЕНТР КАК ОСНОВА НАДЕЖНОСТИ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

В области информационных технологий большую роль играет проблема интероперабельности - взаимодействия систем между собой посредством информационно-коммуникационных технологий. Основная причина возникновения проблемы связанна с повсеместном использовании информационных систем во всех сферах жизни и насыщению разнородными средствами вычислительной техники, что привело к созданию гетерогенной среды, в которой разнородные компоненты должны взаимодействовать друг с другом. Причем уровень гетерогенности с развитием технологий постоянно увеличивается.

Одним из направлений совершенствования технологий взаимодействия корпоративных систем является подход, основанный на базе процессингового центра - дополнительного участника информационно-коммуникативной среды, посредством которого происходит взаимодействие между информационными системами. Основной его задачей является уменьшение количества связей, а также стандартизация входящих и исходящих потоков данных. При использовании процессингового центра в информационно-коммуникативной среде реализуется система топологии звезда, где все участники связанны с центральным узлом. Данное решение позволяет отказаться от непосредственного взаимодействия с другими участниками, тем самым уменьшив количество связей до одной двухсторонней. При этом остается проблема построения оптимальной семантической модели стандартизации данных, которая одновременно должна позволять адекватно описывать данные и быть достаточно лаконичной для передачи через каналы связи.

На основе согласованной модели, при получении однородных данных из различных внешних информационных систем, появляется возможность полностью абстрагироваться от источника данных. В результате, подключение новых систем не будет требовать внесения изменений в существующие, что позволит сократить временные и накладные затраты. Использование данной архитектуры предоставит возможности анализа как самих данных, так и процессов взаимодействия систем. Это позволит контролировать потоки данных, их направление и содержимое.

За счет применения топологии звезды в информационно-коммуникативной среде проявляются все преимущества данной архитектуры. Основным является наличие единой точки сбора и обработки информации, что позволяет легко выявить и предотвратить распространение не корректной или не

безопасной информации. Надежность центрального звена необходимо улучшать, посредством внедрения дополнительного дублирования оборудования и сетевой инфраструктуры, для минимизации времени простоя при возникновении каких либо чрезвычайных ситуаций. Причем необходимо отметить, что поддержание работоспособности и безопасности коммуникационных каналов связи с процессинговым центром станет для коллективного пользователя высоко приоритетной задачей, так как будет единственным методом доступа к информации. Дополнительно, использование одного высоко защищенного канала позволит уменьшить затраты на содержание, обслуживание и защиту информационно-коммуникационной сети. Перспективность и защищённость данного решения подтверждается применением его в банковской сфере, где оно хорошо себя зарекомендовало и подтверждает надёжность использования и развития в других областях жизни.

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

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

При защите информации ограниченного доступа, обрабатываемой в автоматизированных системах (далее - АС), возникает необходимость определения минимального набора требований по защите информации от несанкционированного доступа (далее - НСД). Для определения минимально необходимых требований, в соответствии с действующим нормативным документом «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. требуется провести классификацию АС.Несмотря на то, что данному документу уже более 20 лет, он является действующим. Более того, данный документ обязателен для применения при классификации систем, обрабатывающих конфиденциальную информацию.В соответствии с данным документом, классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию. Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Руководящий документ устанавливает девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархии классов защищенности АС. АС группируются в классы, в зависимости от:

– наличия в АС информации различного уровня конфиденциальности (включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А);

– уровня полномочий субъектов доступа АС на доступ к конфиденциальной информации (включает АС, в которых пользователи имеют одинаковые права доступа / полномочия ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности Группа содержит два класса - 2Б и 2А.);

– режима обработки данных в АС: коллективного или индивидуального (включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А).

Необходимыми исходными данными для проведения классификации конкретной АС, в соответствии с данным руководящим документом, являются:

– перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности. Причем здесь самым важным является именно уровень конфиденциальности, т.к. чем он выше, тем более высокие требования предъявляются к АС;

– перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий. Необходимо определить один пользователь в АС или их несколько. Если пользователь один, то АС определенно относится к 3-ей группе, а требование «размещения информации на носителях одного уровня конфиденциальности» выполняется с применением дополнительных мер из более высокого класса защиты (применением контроля информационных потоков);

– матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС. Для классификации АС вполне достаточно простого понимания —

однопользовательская система или многопользовательская. Разрабатывать матрицу доступа или разрешительную систему доступа на этапе классификации не требуется;

– режим обработки данных в АС. Может повлиять на применение дополнительных требований по защите из более высоких классов, но на определение самого класса защиты не влияет.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации. Для определения класса защиты АС от НСД требуетсяопределить: один пользователь или несколько будут работать в АС;права пользователей; уровень конфиденциальности обрабатываемой в АС информации.Представляя содержание «Руководящего документа» на этапе разработки или реорганизации АС, появляется возможность установить минимальныйнабор требований по защите информации от НСД, достаточный для эффективного функционирования АС, перечень лиц, имеющих доступ к средствам АС и наделить субъектов доступа разрешаемыми полномочиями по отношению к защищаемым информационным ресурсам.

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МОДЕЛЬ ПРОЦЕССА КОНФИГУРИРОВАНИЯ КОМПОНЕНТОВ ЗАЩИТЫ ВСТРОЕННЫХ УСТРОЙСТВ

Встроенные устройства представляют собой элементы сложных информационно-телекоммуникационных систем, функционирующих в не доверенном и потенциально враждебном окружении. Поэтому разработка встроенных устройств является сложной задачей, часто требующей экспертных решений. При этом сложность задачи разработки защищенных встроенных устройств обуславливается различными типами угроз и атак, которым может быть подвержено устройство, а также тем, что на практике вопросы безопасности встроенных устройств обычно рассматриваются на финальной стадии процесса разработки в виде добавления дополнительных функций защиты.

В работе предложена модель процесса конфигурирования компонентов защиты встроенных устройств, применение которой в процессе проектирования устройств будет способствовать разработке безопасных и энергоэффективных программно-аппаратных решений. Данная модель организует поиск наилучших комбинаций компонентов защиты на основе решения оптимизационной задачи с использованием экспертных знаний, эвристик и правил для осуществления многокритериального выбора компонентов защиты. Отличительной особенностью разработанной модели является учет функциональных и нефункциональных характеристик компонентов защиты, ограничений устройства и связей между компонентами с использованием оптимизационного подхода.

Под конфигурацией защиты понимается набор компонентов защиты с определенными функциональными и нефункциональными характеристиками. Цель процесса конфигурирования – определить наиболее эффективную с точки зрения заданных нефункциональных показателей (оптимальную) конфигурацию защиты на основе входных данных об особенностях устройства и возможных компонентах защиты. Фактически, в рамках предложенной модели решается задача дискретной оптимизации на множестве конфигураций с целевой функцией, выражаемой с использованием нефункциональных показателей и ограничений на заданные, как функциональные, так и нефункциональные показатели. В качестве целевой функции решаемой оптимизационной задачи рассматривается упорядоченный набор из нескольких нефункциональных показателей, каждый из которых подвергается либо минимизации, либо максимизации в зависимости от семантики нефункциональной характеристики, лежащей в основе рассматриваемого нефункционального показателя (p1→min/max, p2→min/max, p3→min/max,…). Порядок показателей определяется на основе эвристического подхода.

Упорядочивание альтернатив компонентов защиты производится по степени ухудшения значений их нефункциональных ограничений. Фактически, для каждого нефункционального показателя осуществляется сортировка компонентов защиты. Например, для учета энергопотребления имеющихся разновидностей некоторого программно-аппаратного компонента защиты возможные альтернативы упорядочиваются в соответствии с уменьшением величины потребляемого ими тока (измеряемого в mA).

Порядок учета рассматриваемых нефункциональных ограничений определяется в зависимости от относительной важности каждого из них с использованием предложенной в работе эвристики. Данная эвристика задает общий алгоритм приоритезации нефункциональных ограничений встроенного устройства. По существу, для каждого нефункционального ограничения выделяется набор специфичных функциональных и нефункциональных признаков встроенного устройства, таких как «наличие постоянного источника питания», «возможность замены устройства или аккумулятора без ущерба для предоставляемых им сервисов», «высокая зависимость достижения бизнес-целей устройства от энергоресурсов» и др. Для каждого такого признака предопределено значение ранга (например, с заданием значений от 1 до 3, где 1 – низкая важность, 3 – высокая важность) в зависимости от критичности данного признака для выполнимости заданного нефункционального

ограничения (например, ограничения на ресурс энергопотребления). В результате спецификация целевого встроенного устройства анализируется на предмет наличия у него обозначенных признаков. Для каждого нефункционального ограничения выбирается максимальное значение ранга по всем выявленным у разрабатываемого устройства признакам, в соответствии с которыми происходит упорядочивание уже, собственно, нефункциональных ограничений. При этом ограничения, получившие одинаковые результирующие значения ранга, упорядочиваются между собой согласно порядку, предопределенному экспертно.

Отметим, что при каком-либо изменении спецификации системы или особенностей ее реализации итоговый набор компонентов может изменяться вследствие изменений условий, которые учитывались в процессе выбора компонентов, и поэтому процесс конфигурирования должен проводиться повторно.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и программы фундаментальных исследований ОНИТ РАН (контракт №1.5).

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МЕТОДИКА ОЦЕНКИ РЕСУРСОПОТРЕБЛЕНИЯ КОМПОНЕНТОВ ЗАЩИТЫ ВСТРОЕННЫХ УСТРОЙСТВ

Встроенные устройства определяют как программно-аппаратные устройства, вычислительный процесс которых тесно связан с реакцией на процессы физического окружения и выполняется в рамках некоторой физической платформы, которая, помимо непосредственно вычислительных модулей, включает также модули, взаимодействующие с кибер-физическими объектами окружения. К таким объектам относятся разнообразные сенсоры, силовые приводы, сканеры текстовых, звуковых и других данных, устройства отображения информации, разнообразные коммуникационными и навигационные устройства, бытовые и промышленные устройства нагревания, вентиляции, насосные станции, устройства мониторинга и диагностики и др. Как результат, связи между программной частью устройства, с одной стороны, и аппаратно-техническим окружением, с другой, обуславливают наличие дополнительных ограничений, влияющих существенным образом на процесс проектирования таких устройств. В настоящее время широкое применение на практике получил компонентный подход к проектированию встроенных устройств, реализованный, в том числе в рамках платформ Arduino, Raspberry Pi, Beagle board и операционной системы Android. Фактически, встроенное устройство представляется в виде множества взаимодействующих программных и программно-аппаратных компонентов, большая часть которых в силу специфики встроенных устройств, завязанных в своей работе непосредственно на обеспечение установленных требований защиты.

Предлагаемая в работе методика оценки ресурсопотребления компонентов защиты используется в рамках процессов конфигурирования компонентов защиты встроенных устройств для определения эффективных наборов компонентов защиты, которые должны быть реализованы в рамках механизмов обеспечения информационной безопасности от широкого класса угроз. Методика включает действия по определению нефункциональных ограничений, существенных для проектируемого данного устройства. Источником возможных нефункциональных ограничений является методология MARTE (Modeling and Analysis of Real-Time Embedded Systems), являющаяся де-факто стандартом, разработанным в рамках международного консорциума OMG, где релевантные нефункциональные показатели, характерные для встроенных устройств, специфицированы с использованием языка моделирования UML.

Фактически, MARTE определяет базовую систему понятий, программных и аппаратных характеристик устройств для поддержки процессов спецификации, синтеза, верификации, оценки производительности, количественного анализа и сертификации устройств с использованием специализированных UML-профилей. В частности, в рамках методики используются нефункциональные ограничения, построенные на основе следующих классов доменов знаний: HW_Physical, HW_PowerSupply, HW_StorageManager, HW_Computing, HW_Communication, представленных в рамках методологии MARTE.

Для каждого из приведенных классов производятся, во-первых, формирование показателей на основе нефункциональных свойств для формирования количественных оценок ресурсов устройства, которые требуются для выполнения компонентов защиты и, во-вторых, построение алгоритмов получения значений показателей, используя аналитические подходы, метод экспертных оценок, экспериментальные методы по оценке расходования аппаратных ресурсов различными компонентами защиты.

Вычисление численных значений показателей ресурсопотребления осуществляется с использованием методов программного моделирования, а также аналитически путем поиска и

сопоставления фактических данных о характеристиках компонентов защиты, предоставленных организациями-производителями анализируемых программно- аппаратных компонентов.

Предложенная методика апробирована в процессе проектирования защищенной системы охраны периметра помещения в части реализации функций контроля доступа с использованием одноплатных компьютеров Arduino и набора программных и программно-аппаратных компонентов для нее. На основе количественных данных, являющихся результатом методики выл выбран набор программных и программно-аппаратных компонентов из списков имеющихся альтернатив, применение которых позволило построить защищенную систему, с учетом улучшения ее целевых показателей, в том числе, цены и некоторых показателей ресурсопотребления.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и программы фундаментальных исследований ОНИТ РАН (контракт №1.5).

Дешевых Е.А., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ОБЗОР СРЕДСТВ И ПЛАТФОРМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ ДЛЯ ЗАДАЧ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В докладе анализируются программные платформыдля реализации концепции больших данных, предполагаемые для использования для задач мониторинга информационной безопасности.Основное внимание уделяется трем платформам: Hadoop, Spark иDryad.

Hadoop – основополагающая технология для больших данных. Представляет собой свободно распространяемый набор утилит, библиотек и структур, который позволяет разрабатывать программное обеспечение для масштабируемых, распределенных, надежных вычислений.

Spark – быстрая платформа с открытым исходным кодом для обработки крупномасштабных данных. Запуск программ при использовании данной платформы в 100 раз быстрее, чем в Hadoop в памяти, или в 10 раз быстрее на диске. Платформа также может быть запущена на кластерах Hadoop.

Dryad – платформа для написания параллельных и распределенных программ в масштабе от небольшого кластера до значительного дата-центра.Программная модельDryadоснована на построении направленного ациклического графа для каждой распределенной задачи.Такая реализация дает возможность исполнять большее количество параллельных алгоритмов.

В ходе работы были проанализированы технические методы, актуальность платформ и их характеристики (см. табл.1.).

Таблица 1. Характеристики платформ для больших данных

Платформа	Программная модель	Хранилище данных	Поддерживаемые языки	Среды выполнения
Hadoop	Map/Reduce, Yet Another Resource Negotiator (YARN)	HDFS	Java, PigLatin, HiveQLидругие.	Linux-кластер, Amazon Elastic MapReduce, Microsoft HDInsight to Windows Server, Windows Azure HDInside
Spark	основанана DAG(Directed Acyclic Graph)	HDFS, HBase, JDBC, Cassandra идр.	Scala, Python и Java	Работает на виртуальной машине Java, что позволяет использовать его на Linux, Unix, Windows и Mac
Dryad	основанана DAG	DSC	C++, C#	Кластер Windows HPC Server

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и РНФ (15-1130029).

Доброрадова В.А., Павлова Л.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПРОБЛЕМА АУТЕНТИФИКАЦИИ ОТКРЫТЫХ КЛЮЧЕЙ (ПРОБЛЕМА АУТЕНТИФИКАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ)

В настоящее время большинство пользователей применяют самый легкий способ аутентификации – доступ по паролю, имеющий ряд недостатков с точки зрения безопасности.

Для улучшения системы безопасности и получения возможности выполнения автоматизированных задач по обслуживанию на других машинах, пользователь ПК может использовать SSH аутентификацию на основе открытого ключа, вместо стандартной аутентификации по паролю.

Аутентификация на основе ключей использует два ключа, один "открытый" (публичный ключ), который доступен каждому и второй "закрытый" (секретный ключ), который доступен только владельцу и никому другому.

Для безопасного соединения с помощью SSH аутентификации, необходимо:

1. Сгенерировать пару ключей - секретный и публичный - на локальном компьютере, с которого пользователь будет подключаться. Ключи должны генерироваться для каждого пользователя отдельно. Секретный ключ необходимо сохранить. При сохранении следует учесть, что с помощью этого ключа можно получить доступ ко всем ресурсам, к которым он будет настроен.
2. Подключиться к удаленному серверу и установить открытый ключ
3. Добавить ключ в агент аутентификации на локальом сервере/целевом сервере (верно для современных версий OpenSSH)

Подключение будет производиться в дальнейшем следующим образом:

1. Клиент SSH устанавливает соединение с сервером и передаёт по установленному защищённому соединению имя пользователя вместе с публичным ключом пользователя, взятым из указанного клиенту SSH секретного ключа.
2. Сервер проверяет, имеется ли в файле $HOME/.ssh/authorized_keys заявленного пользователя публичный ключ тождественный присланному. Если такой ключ есть, сервер возвращает клиенту положительный ответ.
3. При получении положительного ответа клиент SSH предлагает пользователю ввести пароль секретного ключа.
4. Если пароль введён правильно и секретный ключ разблокирован, клиент SSH отсылает серверу зашифрованное при помощи секретного ключа специальное сообщение. Хотим обратить внимание на то, что сам секретный ключ не передаётся и не может быть перехвачен.
5. Сервер расшифровывает присланное клиентом сообщение при помощи выбранного ранее публичного ключа и, если расшифровка проходит удачно, предоставляет регламентированный доступ. Технология проверки расшифрованного сообщения основывается на ассиметричном шифровании: информацию зашифрованную секретным ключом можно расшифровать только публичным ключом, но нельзя публичным ключом зашифровать обратно.

Несмотря на очевидные преимущества, основной проблемой использования доступа по ключу является невидимость процесса аутентификации: всего лишь один раз воспользовавшись незакрытым пользователем окном ssh-клиента злоумышленник может внедрить свой публичный ключ.

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРИМЕНЕНИЕ ГРАФОВ ЗАВИСИМОСТЕЙ СЕРВИСОВ В РАМКАХ ЗАДАЧИ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ ДЛЯ ОЦЕНИВАНИЯ КРИТИЧНОСТИ РЕСУРСОВ СИСТЕМЫ И ОБОСНОВАННОГО ВЫБОРА ЗАЩИТНЫХ МЕР

Сервис-ориентированные архитектуры (СОА), включая подвид СОА – веб-ориентированные архитектуры, в настоящее время являются одной из ключевых технологий. В СОА процессы реализуются с помощью сервисов (сервис – это ресурс, предоставляющий возможность выполнения задач, формирующих необходимую функциональность с точки зрения поставщиков и потребителей услуг). Сложность взаимосвязей между сервисами в СОА приводит к тому, что не всегда просто определить как именно та или иная уязвимость информационной системы повлияет на деятельность организации в целом. Для определения того, как распространится ущерб в информационной структуре организации в результате эксплуатации той или иной уязвимости, были разработаны графы зависимостей сервисов.

Граф зависимостей сервисов представляет собой множество сервисов компьютерной сети связанных между собой в соответствии с тем, как свойства безопасности одного сервиса зависят от свойств безопасности другого. Он задается следующим образом: SG=(R, L), где R – множество узлов графа зависимостей сервисов (сервисов), L – множество связей между сервисами. Связь показывает, что свойства безопасности сервиса предка напрямую зависят от свойств безопасности сервиса потомка. Степень зависимости определяется весовой матрицей W.

Модель сервиса R определяется следующим образом: R={T,Cr}, где T – тип сервиса (информационно-технологические активы, порт или программно-аппаратное обеспечение). Cr – критичность сервиса, определяемая трехмерным вектором критичности свойств конфиденциальности, целостности и доступности сервиса для организации.

В данной работе эту модель предлагается использовать для определения точного уровня критичности активов с учетом финансовой важности их защищенности для бизнес-целей организации, и для более точного анализа рисков компьютерных атак. При этом критичность основных бизнес-активов задается их владельцами. Критичность остальных информационно-

технологических активов, программно-аппаратного обеспечения и портов определяется при обходе графа зависимостей сервисов, путем сложения собственной критичности соответствующего сервиса с критичностью сервиса предка, умноженной на степень зависимости свойств безопасности сервиса предка от свойств безопасности сервиса потомка. При определении критичности сервиса учитываются конъюнктивные зависимости (от защищенности сервиса потомка зависит защищенность нескольких сервисов предков). В этом случае критичность сервиса определяется суммарной критичностью сервисов предков, с учетом весовых коэффициентов зависимости. Также учитываются дизъюнктивные зависимости (критичность сервиса предка зависит от защищенности одного из сервисов потомков). В этом случае критичность сервиса предка делится между сервисами потомками.

В дальнейшем полученные оценки критичности активов применяются в традиционной формуле вычисления рисков – риск определяется как произведение критичности актива, вероятности атаки на данный актив и ущерба, наносимого активу в результате успешной реализации атаки. Поскольку критичность сервиса связана с уровнем финансовых потерь организации в случае нарушения его свойств безопасности, полученное значение риска отражает уровень возможных потерь организации до внедрения защитных мер.

При выборе защитных мер учитываются возможные потери организации до внедрения защитных мер, и возможные потери организации после внедрения защитных мер. Возможные потери организации после внедрения защитных мер определяются уровнем риска после реализации защитных мер, стоимостью их реализации, а также побочными потерями, наносимыми организации в результате реализации защитных мер. На основе разницы между потерями до и после реализации защитных мер формируется коэффициент выбора защитных мер, который необходимо максимизировать.

Преимуществами введения модели зависимостей сервисов в процесс выбора защитных мер является возможность определения критичности активов, не представляющих прямой бизнес-ценности для организации, что позволит не упустить узкие места системы при внедрении защитных мер. С другой стороны, учет данных зависимостей позволяет избежать побочного ущерба при реализации контрмер. Кроме того – это формирование прямой зависимости между стоимостью активов для организации и шкалой оценки критичности, что позволяет обосновать необходимость финансовых вложений в реализацию контрмер для защиты активов.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451).

Дубровин Н.Д., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РЕАЛИЗАЦИЯ ПРОТОТИПА НА БАЗЕ HADOOP ДЛЯ АНАЛИЗА БОЛЬШИХ ДАННЫХ

В современных условиях постоянного увеличения объемов и многообразия данных, традиционные системы управления базами данных становятся менее эффективными и неспособны оперативно обрабатывать огромные объемы неструктурированных данных, как это можно сделать, применив технологии больших данных.

Для быстрой обработки и получения результатов, пригодных для восприятия человеком, используется группа инструментов больших данных, один из них – hadoop. Он представляет собой программную платформу, набор библиотек и сервисных программ, позволяющих выполнять распределенные вычисления на кластерах, состоящих из десятков, сотен или тысяч узлов вычислительной сети используя парадигму MapReduce.

Для выявления угроз безопасности в паре с hadoop предлагается использовать систему предотвращения вторжений и аномалий Cisco.Обнаружение угроз и предотвращение вторжений основано на использовании базы сигнатур.CiscoIPSпозволяет эффективно вести журнал учета состояния событий, отправляя оповещения о нарушениях политики безопасности или попытках несанкционированного доступа к системе на мониторинговую станцию. Особенностью данного решения является работа на высоких скоростях до 10 Гбит/сек,

Реализация прототипа:

1. Установка и настройка hadoop в виртуальной среде;
2. Получение слепка данных большого объема из центра обработки данных СПбГУТ им. проф. М.А. Бонч-Бруевича;
3. Анализ и выявление необходимых данных для исследования, например, используя ip-заголовки, поля протоколов TCP, UDP, RTP, RTCP, фильтрации URL-адресов.
4. Обработка данных с использованием базы сигнатур.
5. Сбор логов о данных, представляющих угрозу безопасности сети.

Данный прототип,основанный на использовании технологии больших данных в совокупности с системой Cisco IPS, показывает, что огромные объемы неструктурированных данных можно быстро обработать и выявить наличие угроз безопасности.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и РНФ (15-1130029).

Дудка А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ВОЗМОЖНОСТЕЙ НАПРАВЛЕННОГО МИКРОФОНА И РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕР ПРОТИВОДЕЙСТВИЯ

Целью работы является повышение качества защиты конфиденциальной информации от направленных микрофонов.

Для достижения этой цели поставлены следующие задачи:

– Анализ возможностей направленных микрофонов и особенностей их использования.

– Анализ существующих методов противодействия направленным микрофонам.

– Выбор, обоснование и рассмотрение наилучшего метода противодействия направленным микрофонам.

– Разработка рекомендаций по правильному использованию выбранного метода.

Наилучшим методом является использование генератора акустических помех. Потому что только этот способ даёт абсолютную гарантию конфиденциальности обсуждаемой информации, даже в неподготовленных для переговорах местах.

В работе представлены расчёты остаточного звукового давления при затухании речевого сигнала (на основании ГОСТ 31295.2-2005 Шум. Затухание звука при распространении на местности. Часть 2. Общий метод расчета).

Дудкина О.К.,Копыльцов А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ЭТИЧНЫЙ ХАКЕР – НУЖНА ЛИ ТАКАЯ ПРОФЕССИЯ РОССИИ ТРЕТЬЕГО ТЫСЯЧЕЛЕТИЯ?

В последнее десятилетие активно развивается новое направление профессиональной деятельности в сфере информационной безопасности – этичный хакинг. Существует много разногласий о том, нужна ли такая профессия в России, не угрожает ли развитие этого направления безопасности страны изнутри. На самом деле, это не новое направление, а закономерный и вполне прогнозируемый результат развития информационной безопасности в нашей стране. Сегодняшние 20-30-летние специалисты в области информационной безопасности родились и выросли в 80-90-е годы, тогда же зародилась и выросла вся система информатизации в Российской Федерации. Бытует мнение, что «этичный хакер («whitehathacker») - в прошлом обычный хакер, который продает свои знания в сфере информационных сетей и систем безопасности. А точнее, он взламывает систему, с разрешения владельца и обнаруживает все лазейки, через которые мог бы пробраться хакер. Но на этом его работа не заканчивается, далее слабые места он делает неприступными для злоумышленников. Кто лучше преступника может рассказать о преступлении и предотвратить его?». Однако такая позиция в корне неверна.

Слово «хакер» в нашей стране до сих пор является синонимом вредоносной деятельности, направленной на шантаж собственников интернет-ресурсов и кражу секретной информации. Этичный хакинг – это мотивированный выбор образованных, талантливых программистов, глубоко интересующихся изучением программного кода, всевозможных уязвимостей программного обеспечения и сетевых ресурсов. Человек, нацеленный на осуществление противоправной деятельности в сфере информационных технологий, найдет необходимую для него информацию всегда, она является общедоступной, он не будет заинтересован в совершенствовании и развитии профессиональных навыков в данной области, он реализует свой замысел в любом случае.

Развитие этичного хакинга в России никаким образом не способствует такой преступной деятельности. Наоборот, если рассматривать систему подготовки кадров в Институтах и Университетах МВД России, ежегодно эти учебные заведения выпускают крайне мало специалистов такого узкого профиля. В частности, оперуполномоченных и инженеров Бюро Специальных Технических Мероприятий выпускает Радиотехнический факультет Воронежского Института МВД России. При этом необходимо отметить, что преступность в Российской Федерации достигла такого высокого уровня развития, что информационные технологии все чаще используются как методы и алгоритмы для совершения преступлений, а информационное пространство – как плацдарм для незаконной и, зачастую, безнаказанной деятельности. Решение данной проблемы видится в создании образовательных программ по специальности «Этичный хакер», доступных как гражданскому населению, так и действующим сотрудникам системы МВД, создании жесткой централизованной

системы сертификации вышеуказанных специалистов, а также простого и доступного инструментария для обучения слушателей онлайн на основе вебинарных площадок. Доступность и сертификация знаний в области этичного хакинга, с одной стороны, позволит информировать население о проблемах информационной безопасности, а с другой - даст возможность повышать уровень профессиональной компетентности сотрудникам МВД на местах, без отрыва от профессиональной деятельности.

Таким образом, формирование стандартов и образовательных программ по специальности «Этичный хакер» - необходимая и насущная потребность, это – новый этап в развитии информационного общества в России третьего тысячелетия.

Дятлов О.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет технологии и дизайна

РАЗРАБОТКА XSLT-ШАБЛОНИЗАТОРА НА ОСНОВЕ ПРОТОТИПА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ ЗАЩИТЫ WEB-САЙТА

В докладе рассматривается разработка технологии автоматизированной генерации шаблонов Web-сайтов на основе прототипирования их графических интерфейсов и XSLT-преобразования, обсуждается круг вопросов, связанных с созданием XSLT-шаблонизатора, способного преобразовать прототип графического интерфейса Web-сайта, созданного в среде Gui Machine, программного продукта компании Alee Software, в готовый Web-сайт для последующей его доработки группой Web-программистов. Прототипирование позволяет решить задачу согласования интересов Заказчика и Исполнителя на начальном этапе разработки программного обеспечения. Оно дает возможность снизить проектные риски и издержки по разработке новых технологически сложных изделий, в особенности для приложений с высоким уровнем требований к обеспечению информационной безопасности.

XSLT-шаблонизатор призван облегчить труд Web-дизайнерам и разработчикам сайтов с помощью автоматизации преобразования прототипа графического интерфейса пользователя в шаблон, что определяет новизну и оригинальность данного подхода.

Евневич Е.Л.
Россия, Санкт Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПЕРСОНАЛИЗИРОВАННЫЙ СЕМАНТИЧЕСКИЙ ПОИСК И АНАЛИЗ СОМНИТЕЛЬНОГО КОНТЕНТА

Современный Интернет содержит большие объемы неблагонадежного ресурса, что обусловливает важность поиска и идентификации подозрительного контента. Для осуществления эффективного поиска синтаксический метод не всегда эффективен. В данной работе предложен способ семантического поиска на основе использования базы данных, а именно множества семантических классов русского языка. Персонализированный семантический поиск, навигация и методы получения и анализа контента представляют интерес как средство сужения поиска и повышения релевантности результата в соответствии с предпочтениями пользователя. Для того, чтобы осуществить попытку смыслового поиска в существующих web-документах, необходим предварительный семантический анализ их содержимого, основная цель которого — улучшить структурирование информации в документах. При переходе к семантическому описанию документов происходит сжатие и обобщение информации, что приводит к новому знанию. В то же время семантическое представление информации невозможно без определения закономерностей совместного употребления слов, где значения каждого слова определяется контекстом его использования, т.е. множеством других слов. Проблема вычислимости здесь связана с тем, что значение каждого из слов этого множества в свою очередь определяется собственным контекстом, состоящим из слов, в число которых может попасть и исходное.

Предлагается использовать аппарат онтологий, при этом представление неопределенности, присущей объектам и явлениям реального мира, требует применения не традиционных, а вероятностных онтологий, которые объединяют логический вывод вероятностных представлений с использованием логики первого порядка. При создании профиля применяется вероятностная онтология идентификации пользователя. В качестве шаблона используется референтная архитектура для разработки вероятностных онтологий. Онтологии также обеспечивают системную интероперабельность. Они создают представление семантики области, поддающееся машинной интерпретации, предоставляя таким образом возможность обмена информацией с четко определенным значением. Референтная архитектура для разработки вероятностных онтологий (RAPOD) каталогизирует и определяет процессы и объекты, необходимые для разработки, внедрения и оценки вероятностных онтологий, разработанных для обмена знаниями и неоднократного использования в предметной области.

Одно из интересных для исследования свойств предложенной системы – неограниченная длина поискового запроса, что позволяет осуществлять поиск и сравнение текстов по текстам. Теоретически увеличение размера текста увеличивает точность его семантического анализа и результатов поиска. Для практического использования системы необходимо провести ее объемное тестирование на основе формальных критериев оценки результатов семантического поиска. Кроме того, возможно дополнение существующей базы данных и поиск новых на основе существующих и собственных статистических алгоритмов и метрик.

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

СИНХРОННЫЙ МАГНИТНЫЙ УСКОРИТЕЛЬ МИКРОСПУТНИКОВ

Спутники Земли играют все большую роль в распространении информационных технологий и обеспечении безопасности, среди них значительное место занимают микроспутники, решающие отдельные частные задачи. В докладе рассматривается проблема использования магнитного поля планеты Земля для продления срока службы микроспутников, что стало возможным после появления сверхсильных постоянных магнитов на основе редкоземельных элементов. Принцип действия магнитного ускорителя заключается в том, что на борту спутника устанавливается постоянный магнит, который сориентарован так, чтобы северный полюс постоянного магнита притягивался к южному полюсу планеты, при этом возникает сила, ускоряющая спутник. Если рассмотреть орбиту, проходящую через магнитные полюса планеты, эта сила будет действовать до тех пор пока спутник не достигнет полюса, потом эта сила будет тормозить спутник. Поэтому возникает проблема изменения ориентации постоянного магнита – после пролета над южным полюсом, магнит должен быть повернут на 180 градусов и теперь уже южный полюс магнита будет притягиваться к северному полюсу планеты и т.д.. Так должна работать система синхронизации магнитного ускорителя, информация для определения момента переключения ориентации магнита может поступать извне от наземной системы слежения за спутником. Как показывают расчеты, можно определить весо-габаритные характеристики микроспутника и его орбиты, при которых магнитное ускорение составляет заметную величину и существенно продлевает время существования микроспутника на орбите. Принцип действия синхронного магнитного ускорителя спутника напоминает по аналогии принцип действия синхрофазотрона. Изготовлено устройство для моделирования синхронного магнитного ускорителя для количественного подтверждения эффекта магнитного ускорителя.

Колодин М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРИМЕНЕНИЕ ЛЁГКОЙ ВИРТУАЛИЗАЦИИ И УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ ДЛЯ ОПТИМИЗАЦИИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ И НАДЁЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

При исследовании надёжности и безопасности информационных систем полезно провести эксперименты для получения точных оценок функционирования будущей системы. Для этого, как правило, либо выполняются точные натурные эксперименты, либо проводится моделирование с использованием более или менее точных моделей исследуемой системы и воздействий на неё.

Однако натурный эксперимент часто невозможен, а модели не всегда достаточно точны и подробны. Тем не менее, можно провести моделирование, близкое к натурному, поместив изучаемую систему в изолированное окружение («песочницу») в виртуальной машине или согласованном наборе таких машин, при этом негативные воздействия имитируются путём корректировки параметров или запускаются в такой «песочнице».

Пусть есть система, состоящая из подсистем, для каждой из которых и для всей системы в целом определены наборы входных и выходных параметров; предположим также, что можно построить общие оценочные функции с учётом весов входных и выходных параметров и подсистемы. Целью будет оптимизация параметров системы и подсистем, что означает, в том числе, и изменение структуры основной системы.

Рассмотрим функционирование такой системы во времени. Будем снимать показания выходных параметров системы и всех подсистем. В результате в простом случае получим числовую матрицу, возможно, многомерную. Исследование полученных матриц в реальном времени невозможно либо чрезвычайно ресурсоёмко, поэтому можно применить несколько подходов, а именно,– либо рассчитывать все значение после цикла опытов, либо использовать дополнительное оборудование (компьютеры в локальной сети, занимающиеся обсчётом параметров параллельно с основной работой), либо пойти по компромиссному пути: заменив часть групп параметров на их взвешенные значения, понизить размерность матрицы и допустить изменчивость значений элементов матриц.

Полученные переменные матрицы отличаются от обычных статических: нужно вычислять значения целевых функций при том, что значения параметров постоянно изменяются. Непрерывные

перепроверки изменения параметров слишком ресурсоёмки, прежде всего по времени, поэтому посредством дескрипторов (Python descriptors) строятся минимальные обёртки над объектами-значениями элементов матрицы, вызывающие обращения к подсистеме регистрации изменений, в результате чего получаем матрицу количественных или качественных изменений исследуемой матрицы. Снятие показаний производится так, чтобы инструмент минимально влиял на исследуемую систему. Данные сохраняются только в оперативной памяти и при необходимости пересылаются по локальной сети на вспомогательные машины.

Для оценки безопасности и иных оценок применяются как качественные сигналы (например, изменение параметра, существенное отклонение, ошибка, фатальная ошибка), так и количественные (новые значения либо отклонения от прежних). Исследования касались, прежде всего, работы веб-сайтов, баз данных, настройки параметров вычислительной системы под изменяющиеся требования.

Наиболее интересные результаты получаются при замыкании контура обратной связи, так, что управляющие параметры системы выбираются на основе полученных выходных параметров. При этом управляющая система динамически формирует новые наборы параметров для исследуемой системы, что включает как локальные значения параметров подсистем, так и общие конфигурационные параметры для всей исследуемой системы. Управляющая система при этом пытается подобрать оптимальные в некотором смысле значения таких параметров.

На нынешнем этапе методу присущи некоторые ограничения: недостаточная безопасность самой системы моделирования (контейнерные конфигурации запускаются в режиме суперпользователя), взаимные воздействия подсистем при работе на одном компьютере (но в последних версиях пакетов Docker и Ansible стало удобнее задавать параметры формируемых контейнеров, что позволяет выполнять более точную настройку формируемых конфигураций).

Эксперименты проводились на компьютерной системе в локальной сети со следующими параметрами: на основной машине ОЗУ 16 ГБ, ОС Linux Mint 17.2, Ansible 1.9.3, Docker 1.7.1, СУБД Sqlite 3.8.11.1, Python 3.5 (с веб-движками Flask, Bottle и ORM Peewee, пакетами matplotlib, numpy в составе научного метапакета Anaconda 2.3.0), Golang 1.5.1, IPython, Julia 0.3.11, Redis и RQ; вспомогательные машины имели сопоставимые настройки при меньшем объёме ОЗУ и более слабых ЦПУ (один компьютер использовался для управления процессом, второй – для накопления данных и их обсчёта).

В результате экспериментов было показано, что возможна оптимизация параметров исследуемых систем как статически (между опытами), так и динамически (количественная и качественная, с перестройкой структуры вычислительной системы).

Коломеец М.В., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ВИЗУАЛИЗАЦИЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ С ПОМОЩЬЮ ДИАГРАММЫ ВОРОНОГО

В современных условиях постоянного роста объёма и размерности информации касающейся безопасности, весьма актуальна проблема её эффективной визуализации. Классические визуализационные модели (графики, графы и карты деревьев) часто теряют эффективность при отображении больших объёмов данных или вовсе не могут быть использованы при добавлении новых параметров в отображаемую модель.

При анализе параметров безопасности компьютерных сетей, как правило, используется представление в виде графа, которое, если не считать визуализации топологии, способно эффективно отобразить всего несколько метрик. Представление сети в виде Диаграммы Вороного, способной отображать большее количество параметров и большее количество информации, может повысить эффективность визуализации данных безопасности при анализе компьютерных сетей.

В Диаграмме Вороного вершины графа компьютерной сети представляются в виде плоскостей, соприкосновение которых говорит о наличии связи между ними. Таким образом, благодаря отображению каждого узла сети в виде плоскости, становится возможным использование большего числа метрик, а так же отображения вложенности внутри вершин-плоскостей. Следует отметить, что в Диаграмме Вороного отсутствует неиспользуемое пространство, что также повышает эффективность визуализационной модели.

Процесс построения Диаграммы Вороного состоит из следующих фаз:

1. определение выпуклой оболочки из узлов графа;
2. построение ограниченной триангуляции Делоне с ограничениями в виде существующих рёбер графа и выпуклой оболочки;
3. определение весовых центров получившихся примитивов триангуляции;
4. создание плоскостей на основе весовых центров, примитивы которых имеют общую точку с вершиной начального графа;

5. создание сепараторов на гранях плоскостей, которые не имеют соответствующей связи на начальном графе.

Предполагается, что разрабатываемая визуализационная модель на основе Диаграммы Вороного повысит эффективность отображения информации касающейся безопасности компьютерных сетей как со стороны визуализируемых данных, так и со стороны когнитивных особенностей человеческого восприятия.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451).

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ЛОКАЛЬНОЙ РЕГУЛЯЦИИ КРОВОТОКА

Регуляция кровотока осуществляется на основе информации поступающей от различных органов. Предлагается математическая модель локальной регуляции кровотока и транспорта кислорода в ткани, которая учитывает транспорт кислорода и продуктов метаболизма, а также влияние продуктов метаболизма на диаметр артериол. При моделировании транспорта кислорода из эритроцита в окружающие ткани предполагается, что эритроцит движется прямолинейно и равномерно, в эритроците осуществляется равновесная реакция гемоглобина с кислородом, а в ткани - миоглобина с кислородом. Транспорт кислорода осуществляется из эритроцита через слой (плазму, эндотелий и интерстициальное пространство) в ткань, где кислород поглощается, и выделяются, в ходе биохимических реакций, продукты метаболизма, которые путем диффузии и с потоком крови выводятся из ткани. Транспорт кислорода описывается системой дифференциальных уравнений, которая включает уравнения для эритроцита, для слоя между эритроцитом и тканью и для ткани. При поглощении кислорода тканями выделяются продукты метаболизма, которые диффундируют в ткани и переносятся с током крови к венозной части сосудистого русла.

Таким образом, образование и транспорт продуктов метаболизма в ткани, слое и кровеносных сосудах описывается системой дифференциальных уравнений для ткани, для слоя (интерстициального пространства и эндотелия) и для капилляра. В итоге, уравнения описывают транспорт кислорода и продуктов метаболизма в эритроците, плазме, капиллярном эндотелии, интерстициальном пространстве и ткани. Математическая модель регуляции кровотока и транспорта кислорода в ткани учитывает строение сосудистой сети, включающей артериолы, венулы и капилляры между артериолами и венулами. Кровь протекает последовательно через артериолы, капилляры и венулы. Кровоток в сосудистой системе осуществляется за счет разности давлений на концах сети и описывается законом Пуазейля в артериолах и венулах, а в капиллярах используется обобщенный закон Пуазейля, который учитывает перепады давления на эритроцитах и столбиках плазмы между ними. При поступлении эритроцитов в капиллярное русло кислород выделяется из эритроцитов, диффундирует в ткани и поглощается. В ходе биохимических реакций в тканях происходит выделение продуктов метаболизма, которые выносятся путем диффузии и с током крови в венозное русло. Одна часть продуктов метаболизма поступает с током крови в более крупные вены, а другая - диффундирует в артериолы. Продукты метаболизма, после поступления из венулы в артериолу, воздействует на гладкие мышцы артериолы, и радиус артериолы изменяется. Изменение радиуса артериол приводит к изменению скорости кровотока в сосудах, скорости доставки кислорода в ткани, изменению парциального давления кислорода в ткани, скорости выделения продуктов метаболизма в ткани, изменению их концентрации в венозном и артериальном руслах и, следовательно, радиуса артериол. Таким образом, получилась замкнутая система дифференциальных уравнений, которая решалась на компьютере методом конечных разностей. При исследовании кровотока и транспорта кислорода в ткани наибольший интерес представляет информация, поступающая от интерорецепторов, расположенных в сосудах, поскольку, если информация, поступающая от интерорецепторов, по каким-либо причинам окажется искаженной (или неверной), то это может привести к непоправимым последствиям, например, спазмам сосудов.

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

ОЦЕНИВАНИЕ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ

В последние годы много внимания уделяется обработке слабо формализованной информации, одним из важных показателей которой, является безопасность этой информации и методы ее оценивания. По аналогии с обработкой информации в живом организме, предлагается подход для обработки слабо формализованной информации, поступающей от технических систем. Такой подход, реализованный в виде обобщенного алгоритма, обладает следующим набором функциональных возможностей: оценивание достоверности поступающей информации, оценивание безопасности

поступающей информации, оценивание вероятности, с которой можно доверять поступающей информации, выработка устойчивой реакции на поступающую информацию, поддержка принятия решений и генерация новой информации.

Выбор вышеперечисленных функциональных возможностей обусловлен тем, что эти функциональные возможности выбраны по аналогии с функциональными возможностями живых организмов, и эти функциональные возможности обеспечивают выживание популяций живых организмов во враждебной окружающей среде.

В каждой конкретной задаче перечисленные функциональные возможности возможно изменить (либо сократить, либо добавить новые). Вышеперечисленные функциональные возможности призваны решать следующие задачи. Функциональная возможность «Оценивание достоверности поступающей слабо формализованной информации» решает задачу по аналогии с живой природой, об оценивании достоверности информации. Если информация достоверная, то ее нужно учитывать и в случае необходимости на нее каким тот образом реагировать, а если недостоверная, то нет. Функциональная возможность «Оценивание безопасности поступающей слабо формализованной информации» решает задачу по аналогии с живой природой, об оценивании безопасности информации.

Если информация представляет опасность, то ее нужно учитывать и в случае необходимости на нее каким тот образом реагировать, а если безопасная, то нет. Функциональная возможность «Оценивание вероятности, с которой можно доверять поступающей слабо формализованной информации» решает задачу по аналогии с живой природой, об оценивании вероятности, с которой можно доверять поступающей слабо формализованной информации.

Если вероятность велика, то ее нужно учитывать и в случае необходимости на нее каким тот образом реагировать, а если невелика, то нет. Функциональная возможность «Выработка устойчивой реакции на поступающую слабо формализованную информацию» решает задачу по аналогии с живой природой, о выработке условных рефлексов. Если какая-либо информация поступала прежде и реакция на эту информацию приводила к выживанию живого организма, то эта информация и поведение живого организма после получения этой информации запоминается.

При неоднократном поступлении такой информации вырабатывается условный рефлекс. Функциональная возможность «Поддержка принятия решений» решает задачу по аналогии с живой природой, о поддержке решений живого организма с целью выживания (заботиться о питании, избегать опасностей и т.д.). Функциональная возможность «Генерация новой информации» решает задачу по аналогии с живой природой, о генерации новой информации на основе личного опыта, поскольку от этого зависит существование организма (живой организм должен осваивать и вырабатывать свои собственные способы добычи пропитания, избегания опасностей и т.д.). Для обработки слабо формализованной информации могут быть использованы распределенные информационно-вычислительные системы или кластеры высокопроизводительных параллельных вычислений.

Крылов К.Ю., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

АНАЛИЗ МЕТОДИК ПРИМЕНЕНИЯ КОНЦЕПЦИИ БОЛЬШИХ ДАННЫХ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

На сегодняшний день актуальной проблемой использования компьютерных сетей является обеспечение их комплексной безопасности. Традиционный подход к обеспечению сетевой безопасности построен на стратегиях защиты периметра сети, однако в соответствии с современными концепциями защиты данный подход устарел, так как механизмы защиты компьютерных сетей должны быть реализованы в различных точках сети.

Важнейшим механизмом, на который опирается реализация данного подхода, является мониторинг безопасности сети. Одним из вариантов обеспечения безопасности является модель нулевого доверия (Zero-Trust Model, ZTM). Этот подход предполагает установление контроля за всеми данными сети, исходя из предположения, что каждый элемент сети (например, файл) таит в себе потенциальную угрозу.

Мониторинг безопасности сети, основанный на использовании ZTM-модели, обуславливает необходимость обработки огромных объемов данных в реальном времени и их хранения. Анализ логов, сетевых пакетов и системных событий и другой релевантной информации для обнаружения угроз и вторжений является серьезной проблемой и традиционные технологии не в состоянии обеспечить выполнение задач реализации обработки этой информации по нескольким причинам:

– хранение большого количества данных экономически не целесообразно. В результате, большинство логов событий и другая записанная компьютерная деятельность удаляются после фиксированного периода хранения (например, 60 дней);

– выполнение сложных запросов на больших, структурированных наборах данных - неэффективно, потому что традиционные инструменты не используют технологии больших данных;

– традиционные инструменты не предназначены для анализа и управления неструктурированными данными; инструменты больших данных (например, скрипты и регулярные выражения) могут запрашивать данные в гибких форматах;

– системы обработки больших данных используют кластерные вычислительные инфраструктуры; в результате, эти системы более надежны, доступны и экономичны.

В докладе раскрываются вопросы применения концепции больших данных для мониторинга безопасности компьютерной сети. Рассматриваются различные методики, базирующиеся на концепции больших данных, такие как Hadoop, Spark, MapReduce, Dryad, позволяющие хранить и анализировать большие наборы гетерогенных данных.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) и РНФ (15-1130029).

Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

АРХИТЕКТУРАСИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В ПОМЕЩЕНИЯ НА ОСНОВЕ БЕСКОНТАКТНЫХ СМАРТ-КАРТ

В настоящее время встроенные устройства получают все большее распространение в самых разных областях приложения − в системах управления и контроля на транспорте, в системах управления производственным процессом, системах, предоставляющих телекоммуникационные сервисы потребителям, в системах имплантируемых медицинских устройств для контроля жизненно важных показаний организма человека, в электроэнергетике, в системах обеспечения физической безопасности помещений, прикладных системах распознавания речи и др.

Критически важный характер таких систем, а также высокая степень взаимодействия встроенного устройства с другими элементами программно-аппаратного окружения и пользователями системы обуславливает важность разработки механизмов защиты таких устройств от угроз информационной безопасности.

На основе установленных требований к защите с учетом ограничений устройств и связей между компонентами необходимо решить вопрос комбинирования компонентов встроенных устройств. Под компонентами понимаются программные и программно-аппаратные компоненты, которые интегрируются в устройство для реализации некоторого функционального требования защиты. Например, функциональное требование "поддержка беспроводного канала передачи данных" реализуется путем использования микроконтроллера со встроенной антенной или поддерживающего соответствующие расширения.

Разработка системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт подразумевает соответствие системы ряду функциональных требований, а также оптимальность системы с точки зрения нефункциональных требований (энергоэффективность, стоимость, занимаемое пространство). В соответствии с функциональными требованиями,были сформированы наборы компонентов защиты на базе микроконтроллеров Arduino, Raspberry Pi, Beaglebone BlackиIntel Galileo. Полученные наборы были проанализированы по нефункциональным требованиям с целью выявления оптимального. Таким набором стал набор компонентов защиты на базе микроконтроллера Arduino Yun.

Полученный набор компонентов защиты стал основой системы контроля и управления доступом в помещение на основе бесконтактных смарт-карт.

Архитектура системы содержит следующие компоненты:

1) встроенное устройство,

2) сервер управления доступом,

3) сервер журналирования,

4) клиент администратора, для управления информацией, хранящейся в базе сервера управления доступом,

5) клиент, для журналирования начала и завершения сеанса пользователя с операционной системой.

В дальнейшем, система будет использоваться в качестве стенда для отработки векторов атак в рамках концепции интернета вещей, а журнальные записи, собираемые при работе системы, будут подвергнуты процессу корреляции событий безопасности для выявления причинно-следственных связей.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451, 15-37-51126).

Марков А.С., Фадин А.А.
Россия, Москва, ЗАО «НПО «Эшелон»

РЕАЛИЗАЦИОННЫЕ ОСНОВЫ СИГНАТУРНО-ЭВРИСТИЧЕСКОГО АНАЛИЗА БЕЗОПАСНОСТИ ПРОГРАММ

Большой объем, сложность и динамизм обновлений современного программного кода и объективное наличие в нем ошибок и уязвимостей определяет ряд проблемных задач в области обеспечения информационной безопасности компьютерных систем. Использование автоматизированных средств аудита безопасности программного кода позволяет повысить эффективность работы эксперта за счёт локализации потенциально опасных фрагментов программного кода. В частности, применение статических анализаторов исходных текстов программного обеспечения (ПО) позволяет проводить аудит безопасности программного кода в приемлемые сроки.

Среди средств статического анализа на практике применяются как коммерческие продукты (AppChecker, Appercut, CppCat), так и продукты с открытыми исходными текстами (CppCheck, PDM, Rats). Авторы проанализировали инструменты статического анализа исходных текстов согласно проектам NIST SP 500-268 и SATEC (формирующим наборы требований к функциональным особенностям анализаторов), а также согласно к классам обнаруживаемых дефектов. Важными критериями при анализе статических анализаторов являются наличие соответствия обнаруженных дефектов различным классификациям, функционал по работе с ложно позитивными срабатываниями и возможность совместной работы нескольких экспертов в системе. Особое внимание уделялось на возможности инструментов статического анализа по предоставлению результатов работы, как наиболее востребованные аудиторами исходных текстов в своей работе.

Сравнение показало, что большинство анализаторов предоставляет возможность конфигурировать, группировать и создавать свои правила анализа, формировать отчеты в форматах HTML и XML, настраивать и сохранять фильтры ложных срабатываний. Помимо перечисленных возможностей, только ApperCut и AppChecker опираются на известный стандарт CWE, являющийся открытым, исчерпывающим источником информации о дефектах. Средства CppCat и CppCheck позволяют проводить инспекцию найденных потенциально опасных конструкций кода ещё до завершения анализа, что способствует более продуктивной работе.

При анализе проектов, содержащих большие объёмы исходных текстов, на первый план выходят возможности по совместной работе нескольких экспертов над одним проектом, а так же возможности по одновременному анализу нескольких проектов. В полной мере этим требованиям удовлетворяют продукты AppChecker и ApperCut.

Необходимо упомянуть, что длительность анализа является результатом компромисса между точностью, глубиной и масштабируемостью применяемых механизмов анализа. Большинство анализаторов используют упрощения и эвристические алгоритмы для уменьшения времени анализа.

Эвристический анализ представляет поиск дефектов в программном коде, сравнивая фрагменты кода с образцами из базы данных дефектов безопасности (эвристические правила). Эксперт дает окончательное заключение о критичности дефекта и возможности его эксплуатации злоумышленниками. Эксплуатируемый дефект безопасности представляет собой уязвимость, которая представляет угрозу информационной безопасности.

Для повышения унификации обнаружения стандартных дефектов и уязвимостей авторами предлагается использовать многоуровневую модель эвристического анализа, так как она обеспечивает обнаружение дефектов для таких вариантов исходного кода, как:

- лексический код;
- синтаксическое дерево;
- дерево Кантаровича (абстрактное синтаксическое дерево, AST);
- граф потока управления (CFG);
- граф потока данных (DFG);
- SSA-представление;
- абстрактный семантический граф (ASG).

Для формализации обнаружения дефектов кода авторы предлагают использовать продукционную модель представления знаний, так как она является легкой для понимания и применения, с учетом того, что в настоящее время известны не более 100 классов критических дефектов для определенного языка программирования.

Заключение. Обнаружение дефектов программного кода является одной из важнейших задач информационной безопасности. Применение современных статических анализаторов с использованием метода сигнатурно-эвристического анализа позволяет не только обеспечить полноту проверок, а также значительно повысить качество анализа и уменьшить время его проведения.

Михайлов Н.С.
Россия, Санкт-Петербург, АО «Равенство»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ДОСТУПА ВПРОГРАММНЫЕ МОДУЛИ ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Обеспечение безопасного доступа в программные модули интегрированной корпоративной информационной системы (КИС) необходимо для контроля доступа пользователй к различной информации, имеющейся в КИС. Важно не допустить пользователей к конфендициальной информации, не обладающих требуемым уровнем прав. Сложность решения данной проблемы возрастает с ростом количества модулей КИС. Информация, хранящаяся в интегрированной базе данных, может быть получена пользователемя из разных модулей. При этом программные модули интегрированной КИС могут иметь собственные системы разграничения прав доступа, что усложняет вычисление «суммарных» прав пользователя.

При разработке общей модели уровней доступа пользователей интегрированной КИС следует учитывать указанные особенности и обеспечить контроль над получением информации из различных программных модулей. Одним из способов решения этой задачи является механизм синхронизации пользователей и контроля смежных прав доступа на уровне промежуточного программного обеспечения.

Михайлова А.С.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

СРЕДСТВА БЕЗОПАСНОГО ДОСТУПА ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТЕЗАУРУСА ТЕКСТОВОЙ ИНФОРМАЦИИ

Информация, содержащаяся в тезаурусе, может быть доступна по сети большому числу пользователей. Поэтому при разработке тезауруса для обеспечения целостности и сохранности информации, необходимо разработать меры безопасности.

Было предпринято довольно много успешных попыток частично автоматизировать процесс построения тезауруса. К недостаткам существующих методов можно отнести следующие:

1. Значительные временные затраты.
2. Ограничение применения тезауруса, в основном для индексации и классификации ресурсов.
3. Использование интуитивных методов исследования при формировании тезауруса.
4. Установление связей между понятиями производится вручную и единожды одним экспертом.
5. Различие мнений нескольких экспертов, одного эксперта по всем предметным областям не существует.
6. Невозможность одновременной многопользовательской работы с системой.

С учетом вышеперечисленных недостатков, был предложен метод автоматизированного построения тезауруса, основанный на онтологической модели представления текстовой информации, имеющей количественную характеристику связей между элементами.

Передача информации из тезауруса текстовой информации клиенту должна происходить по протоколам с необходимым уровнем защиты. Если требуется ограничить доступ пользователей к тезаурусу, то необходимо проводить их авторизацию вплоть до уровней полномочий. Уровни полномочий могут разделяться в зависимости от статуса пользователя тезауруса: частичный или полный просмотр, изменение информации и другие.

Не стоит забывать и о безопасности физических устройств (жесткие диски, сервера и т.п.), хранящих информацию тезауруса.

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

ОРГАНИЗАЦИЯ ОБМАННЫХ ЛОВУШЕК В АЛГОРИТМАХ ОТРИЦАЕМОГО ШИФРОВАНИЯ С РАЗДЕЛЯЕМЫМ СЕКРЕТНЫМ КЛЮЧОМ

Обеспечение стойкости шифрования информации в условиях атак с принуждением относится к задачам отрицаемого шифрования. При атаке с принуждением воздействие противника направлено на отправители или получателя с принуждением отправителя или получателя раскрыть параметры шифрования или расшифрования. Стойкость к атакам в подобных случаях обеспечивается алгоритмами отрицаемого шифрования. Криптограмма строится из некоторых осмысленных исходных сообщений, и/или получением из криптограммы различных расшифрованных текстов. Атакующему передаются параметры шифрования, связывающие криптограмму с определенным фиктивным текстом. Атакующий проверяет сообщение, удостоверяется, что использование параметров приводит к преобразованию сообщения (фиктивного) в заданную криптограмму. Алгоритм отрицаемого шифрования будет считается стойким, если результат проверки проявит себя как положительный.

Механизм защиты исходной информации по типу обманных ловушек использует механизмы способов отрицаемого шифрования, которые дают возможность достаточно быстро совместно зашифровать два и более различных сообщений на двух или более различных ключах конечной длины. Одно из сообщений будет фиктивным и зашифровывается на фиктивном секретном ключе, к нему организуется контролируемый доступ нарушителя - ловушка.

При расшифровании составленного фиктивного сообщения нарушитель оказывается введенным в заблуждение. Устанавливается предположение, что нарушителю известен алгоритм расшифрования санкционированного пользователя, и нарушитель может проанализировать криптограмму с ее использованием при выполнении процедуры расшифрования по фиктивному ключу. Организация ловушки не должна дать обоснованных подозрений, что кроме существования полученного им фиктивного ключа имеется некоторый другой ключ, позволяющий расшифровать криптограмму в другое осмысленное сообщение. Организация обманных ловушек в алгоритмах отрицаемого шифрования построена так, что не позволяет атакующему отличить процедуру отрицаемого шифрования от вероятностного шифрования по криптограмме, по фиктивному сообщению и по фиктивному ключу.

Организация ловушки предопределяет требования к алгоритмам отрицаемого шифрования:

1. алгоритмам обеспечивает неотличимость отрицаемого шифрования по криптограмме от вероятностного шифрования;
2. алгоритм организует одинаковость процедур расшифрования для различных используемых ключей;
3. алгоритм предполагает идентичность использования (равноправность) всех битов криптограммы для всех возможных значений ключа расшифрования.

Шифрование сообщения представляется в виде последовательности битовых знаков.На каждом шаге зашифрования значения сообщений выбираются по случайному закону и путем подбора значений, т.е. эти процедуры являются вероятностными и обладают универсальными и оригинальными особенностями:

1. любая хэш-функция или блочное преобразование может быть использовано для реализации вероятностного шифрования по этому способу,
2. полное совпадение формул зашифрования и расшифрования,
3. возможность выполнения одновременного зашифрования двух и более сообщений.

Вместо хэш-функции шифрования можно использовать алгоритм блочного шифрования. В случае использования алгоритмов блочного шифрования, включение счетчика в аргумент также улучшает статистические свойства отрицаемого шифрования. Преимущество использования блочных шифров в сравнении с использованием хэш-функций заключается в том, что выходное значение блочных шифров имеет меньшую длину, благодаря чему достигается более высокая производительность алгоритма отрицаемого шифрования. При использовании в процедуре отрицаемого шифрования блочного шифра как в режиме шифрования, так и в режиме расшифрования (ассоциированные вероятностные шифры по фиктивному ключу), предложенный способ обеспечивает построение алгоритмов отрицаемого шифрования, обладающих скоростью шифрования в 100 и более раз высокой по сравнению с алгоритмами, построенными на основе хэш-функции.

Применение алгоритмов отрицаемого шифрования с разделяемым секретным ключом в качестве механизма защиты информации позволяют реализовать защиту по типу организации обманных ловушек, сформулированы требования к алгоритмам этого типа, описаны разработанные способы и конкретные алгоритмы отрицаемого шифрования, удовлетворяющие сформулированным требованиям. Применение разработанных алгоритмов с указанием ассоциированного вероятностного шифра интересного тем, что в процессе расшифрования криптограммы случайные значения, использованные при выполнении процедуры зашифрования, не восстанавливаются однозначно, в отличие от известных вероятностных блочных шифров, когда в процессе расшифрования использованные случайные значения восстанавливаются однозначно. Это определяет самостоятельный интерес к рассмотренным алгоритмам вероятностного шифрования с разделяемым секретным ключом.

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

ВИЗУАЛЬНЫЙ АНАЛИЗ ИЗМЕНЕНИЯ ПАТТЕРНОВ ДАННЫХ В ПОТОКАХ ДАННЫХ БОЛЬШОГО РАЗМЕРА

Увеличение объемов потоков данных от различных измерительных устройств, сообщений из социальных сетей, устройств сотовой связи, аудио- и видео-регистрации обуславливают необходимость разработки методов обработки анализа многообразных структурированных и неструктурированных данных огромного объема. Одним из возможных способов обработки является

применение методов визуальной аналитики, сочетающих вычислительную эффективность автоматизированных методов интеллектуального анализа данных и способность человеческого мозга выявлять графические паттерны и аномалии. Предлагается подход к исследованию потока данных с временной шкалой, основанный на применении методов поиска часто встречаемых последовательностей объектов и динамической визуализации выявленных паттернов атрибутов объектов в потоке.

Проблема поиска часто встречаемых последовательностей в потоке данных стала классической задачей анализа данных, первым этапом задачи построения ассоциативных правил. Результатом применения метода поиска часто встречаемых последовательностей к потоку данных является определение паттернов различного типа – формирование множества наиболее часто встречаемых объектов, выявление последовательностей или подграфов объектов. Таким образом, этот метод позволяет понять аналитику: что происходит в потоке данных, как меняются его основные характеристики во времени. На основе выявленных последовательностей атрибутов объектов могут быть сформированы динамические паттерны данных, которые могут быть использованы для профилирования потока и прогнозирования возможных изменений в нем. Например, при исследовании сетевых данных метод может определить, что большое число сетевых потоков имеют общий IP-адрес источника, порт назначение и размер потока. Это множество атрибутов может быть положено в основу паттерна сетевой атаки, использующей сканирование портов. Подобные шаблоны могут быть построены для различных видов инфраструктурных атак, и, соответственно, их наличие в потоке данных может свидетельствовать об аномальной активности в сети.

Очевидным преимуществом использования метода поиска часто встречаемых последовательностей является значительное снижение размерности контролируемых данных. Исследования показали, что для множества сетевых потоков размерностью более 40 миллионов при выборе минимального уровня поддержки равным 5%, формируется порядка 10 - 20 последовательностей атрибутов. Следовательно, таким образом, решается одна из основных проблем визуализации исходных данных большого объема – снижение их размерности, и, как результат, построение четкой картинки, легко читаемой пользователем.

В проводимом исследовании предложено представление паттерна данных в виде связного графа, вершинами которого являются атрибуты, входящие в его состав, а также специальная вершина, характеризующая его частоту встречаемости в потоке. В результате применения метода поиска часто встречаемых последовательностей к потоку данных, происходит перестроение паттернов, сформированных на предыдущем интервале времени. Можно выделить следующие переходные состояния паттерна: 1) появление паттерна; 2) исчезновение паттерна; 3) добавление нового атрибута; 4) исчезновение атрибута из последовательности; 4) слияние паттернов; 5) разделение на паттерны. Выявленные изменения предлагается выделять цветом, например, в случае появления новых атрибутов или нового паттерна; или прозрачностью цвета, например, в случае исчезновения паттернов, атрибутов. Слияние паттернов и их разделение может быть отражено форматом и цветом линии, соединяющей соответствующие атрибуты. Такое графическое представление легко позволяет отобразить предыдущее состояние паттерна / паттернов, и при этом восприятие генерируемого изображения не затрудняется. Исследование динамики изменения паттернов данных за достаточно длительный период времени требует поиска других графических представлений. Имеются решения, в основе которых лежит стопочная диаграмма, однако такое представление не отражает структуру паттерна. Для устранения этого недостатка предлагается использовать стопочную диаграмму в сочетании с предложенным выше графическим представлением паттерна, при этом выделение элемента диаграммы должно сопровождаться детальным представлением паттерна в виде связного графа.

Дальнейшие исследования, связанны с анализом эффективности предлагаемого подхода к исследуемому потоку данных большого размера.

Новожилов Д.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ПОДДЕРЖКИ ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТОВ ПО КЛАССИФИКАЦИИ ВЕБ-САЙТОВ

Нынешний этап развития цивилизации характеризуется небывалым количеством информации, доступной пользователям по всему миру, основным источником которой служит Глобальная Сеть Интернет. Однако далеко не все эти сведения можно считать полезными. Часть размещенного во Всемирной паутине содержимого является неприемлемым, вследствие чего возникает необходимость защиты от информации и блокировки вредоносного контента. Данные задачи находят свое решение в различных системах автоматической классификации веб-сайтов, например, в системах родительского контроля. Один из подходов к построению подобных систем заключается в

использовании методов Data Mining с целью построения классификатора, который будет на основе различных признаков определять принадлежность веб-страницы к той или иной категории.

В ходе проведения экспериментов в данном направлении, ввиду участившихся ошибок и неточностей, возникла необходимость изменения и доработки используемых средств сбора и подготовки данных. Подобное решение продиктовано чрезвычайной важностью подготовительных стадий во всем процессе исследований: во многих случаях именно они занимают значительное время. К другим существующим проблемам можно отнести большую трудоемкость, возрастающую с добавлением новых признаков, и недостаточную степень автоматизации на данных этапах, требующую от человека-оператора контроля за ходом процессов и выполнения вручную некоторых промежуточных действий. Один из возможных выходов из сложившейся ситуации - разработка комплекса программных средств поддержки проведения экспериментов.

Среди задач, стоящих перед создаваемой системой, наиболее важными являются: сокращение затрат времени при подготовке исследований, автоматизация процесса сбора данных и повышение удобства работы.

На основе анализа возможных способов построения системы было решено представить её архитектуру в виде набора программных модулей с четко определенными входами и выходами, последовательная работа которых и будет обеспечивать весь процесс подготовки экспериментов. Кроме того, необходимо предусмотреть варианты, когда те или иные модули будут пропущены (например, если необходимо уточнить те или иные промежуточные данные или изменить условия эксперимента). Таким образом, акцент делается на гибкости и возможности многократного использования.

Первый модуль в системе обеспечивает загрузку категоризированных списков сайтов (URLBlacklist, Shalla's Blacklist, DMOZ) из Интернета. Далее производится распаковка скачанного архива, после чего его содержимое помещается следующим модулем в базу данных. Затем следует этап многопоточной загрузки, на котором возможно сохранение изображений с веб-сайтов и исходников страниц (как с учетом динамического содержимого, генерируемого в браузерах с помощью JavaScript, так и без него: только HTML). На следующем этапе извлекаются признаки для анализа: текстовые (полный текст веб-страницы и текст, извлеченный из HTML-тэгов, например, содержимое <meta>); структурные (статистика HTML-тэгов); URL-страницы (для последующего анализа N-грамм); изображения и данные Whois-серверов. После чего выбранные признаки преобразуются в формат, используемый ПО анализа данных RapidMiner (.dat и .aml). В зависимости от особенностей эксперимента (выбранных признаков, количества категорий классификации) выполняется подстройка схемы работы для RapidMiner, сохраненной в виде шаблона, под конкретные условия.

В соответствии с выбранной схемой, RapidMiner выполняет построение моделей и обучение классификаторов. Промежуточные результаты сохраняются на жесткий диск блоком Write Model, а затем считываются в процессе выполнения схемы, что позволяет снять возможные проблемы, возникающие вследствие ограниченности объемов оперативной памяти. По этой же причине RapidMiner управляется из командной строки, без загрузки основного интерфейса. Заключительными шагами являются оценка результатов эксперимента и генерация отчетов, отображаемых в каком-либо приложении. При этом предполагается, что все модули будут объединены с помощью единого пользовательского интерфейса, который позволит задавать параметры и выбирать те из модулей, которые будет необходимо запустить. Также должны быть предусмотрены файлы конфигурации и ключи командной строки для случаев запуска без использования оконного интерфейса.

Для обеспечения удобства проведения экспериментов необходимо предусмотреть наложение ограничений на исходные данные (например, задание минимального размера текстового содержимого, выбор используемых для классификации категорий и основного языка анализируемых веб-сайтов). Другой отличительной особенностью должна стать структура программного кода, предусматривающая возможность легкого расширения функциональности, например, при добавлении новых списков категоризированных сайтов или признаков для анализа.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451).

ПервухинаЕ.Л., ОсиповК.Н., ТимофеевИ.
Россия, Севастополь, Севастопольский государственный университет

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ УПРАВЛЕНИЯ ПРИЕМОСДАТОЧНЫМИ ИСПЫТАНИЯМИ ДВС

Задачи совершенствования технологического процесса производственных испытаний современных изделий машиностроения по-прежнему актуальны. Решение указанных задач неразрывно связанно с совершенствованием систем измерения, обработки, хранения и передачи различной информации, получаемой в ходе испытаний, а также с разработкой новых подходов к управлению процессом испытаний. Очевидно, что создание автоматизированных рабочих мест с

централизованной базой данных, а также современные средства корпоративного шпионажа, обусловленные высокой конкуренцией, объясняют также актуальность задач, связанных с защитой информации.Рассматриваются вопросы, связанные с определением наилучших, с точки зрения установленных критериев, законов управления испытаниями, как части математического обеспечения информационной системы управления производственными испытаниями современных машиностроительных изделий.

Современный условия глобализации и конкуренции ставят перед производителями ДВС задачи создания распределенных корпоративных сетей, для быстрого и безопасного обмена данными, в том числе обмена и обработки данных, касающихся приемосдаточных испытаний выпускаемой продукции. Как правило, такие сети являются весьма обширными и при этом должны отвечать высоким стандартам безопасности.

Широко распространенный способ создания подобной защищенной сети – использование виртуальной частной сети (VPN).Сеть VPNне требует никаких дополнительных коммуникационных линий связи, разворачиваются поверх любой другой сети. Для распределения вычислительных нагрузок, связанных с обработкой данных, полученных в результате испытаний ДВС, современные приложения разрабатываются под использование в интернете, что, в свою очередь, обуславливает применение защищенного протокола прикладного уровня HTTPS, который использует криптографические протоколы для шифрования передаваемых данных. Помимо безопасности сетевого стека технологий, немалая криптографическая устойчивость требуется и от самого веб приложения для предотвращения кражи либо изменения наиболее чувствительной информации, касающейся приемосдаточных испытаний.

Проноза А.А., Чечулин А.А., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»

МОДЕЛЬ ПРЕДСТАВЛЕНИЯ ДАННЫХ РАЗНОРОДНОЙ СТРУКТУРЫ ОБ ИНФОРМАЦИОННЫХ ОБЪЕКТАХ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ ПОДСИСТЕМЫ ВИЗУАЛИЗАЦИИ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ И ИНФОРМАЦИЕЙ БЕЗОПАСНОСТИ

Для современных компьютерных систем характерен высокий рост числа объектов компьютерной инфраструктуры, таких как рабочие станции, сервера, терминалы, коммуникационное оборудование и т.д. Каждый элемент системы порождает собственные сообщения безопасности. Количество таких сообщений стремительно растет вместе с ростом объектов компьютерной сети. Возникает естественная проблема сбора большого потока информационных сообщений, их хранения, обработки и последующая визуализации результатов.Концептуальным решением этой проблемы в части касающейся представления данных разнородной структуры в системах управления событиями и информацией безопасности (SecurityInformationandEventManagement, SIEM) может быть следующий подход.

С точки зрения математических моделей, компьютерная сеть представляет собой связную систему разнородных источников информации. Каждый источник информации генерирует сообщения безопасности, которые поступают на модуль сбора данных SIEM-системы и проходят процедуру нормирования и понижения размерности. В результате получается набор данных разнородной структуры об информационных объектах. В настоящей работе предлагается математическая модель, предназначенная для структурирования указанных данных.

Предлагаемая модель основывается на разработанной классификации типов связей между отдельными сетевыми объектами компьютерной сети. Данная классификация выделяет шесть типов связей: 1) отношения физической связи, 2) отношения доступности, 3) отношения посредством виртуальных каналов связи, 4) отношение функциональной зависимости, 5) отношения доверия и 6) отношения уязвимости. Внутри SIEM-системы установление факта наличия связи между двумя узлами осуществляется в автоматизированном режиме на основеанализа отчетов средств сбора информации и соответствующих событий безопасности.

Таким образом, компьютерная сеть представляется в виде кортежей, каждый из которых состоит из двух информационных объектов и типа отношений между ними. Совокупность всех кортежей составляет многомерную матрицу связей между информационными объектами, в которой для любых двух информационных объектов и типу связи сопоставляется «1», если такой тип связи присутствует между объектами, и «0» в противном случае.Полученная матрица является моделью представления данных разнородной структуры об информационных объектах и может быть использована в качестве массива исходных данных для их визуализации.

Для визуализации компьютерных сетей очень часто прибегают к использованию графа как к наиболее универсальной структуре данных, способной естественно отобразить компьютерную сеть с произвольным числом узлов. Известно, что одним из способов задания графа является двумерная матрица смежности. Чтобы отобразить граф, соответствующий компьютерной сети, сведения о которой содержатся в построенной многомерной матрице, необходимо рассмотреть один из ее

срезов по типу хранящейся в ней связи. Например, чтобы получить матрицу смежности, представляющую топологию компьютерной сети, необходимо получить срез многомерной матрицы связей по наличию физической связи между узлами. Рассматривая срезы по другим видам отношений между узлами можно также получить матрицы смежности для графа доступности, графа защищенных каналов, графа зависимостей, графа доверия и графа атак.

Предложенная модель обладает рядом преимуществ. Во-первых, такая модель позволяет хранить данные обо всех связях информационных объектов компьютерной инфраструктуры единообразно в строго структурированном виде. Во-вторых, с помощью указанной модели можно исследовать всю инфраструктуру сети и под разными углами посмотреть на состояние безопасности тех или иных объектов. В третьих, представленная в модели информация может быть легко визуализирована при помощи графовых и иерархических структур.

Работавыполненаприфинансовойподдержке Министерства образования и науки Российской Федерации (контракт № 14.604.21.0137, уникальный идентификатор RFMEFI60414X0137).

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

ГЕОЛОКАЦИЯ ДЛЯ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ДАННЫХ

В свете увеличивающегося значения геополитики в глобальной сети Интернет появляются востребованные инструменты контроля перемещения данных, которые используют в информационном пространстве понятия «геолокация», «геоограждение» и позволяют осуществлять мониторинг и контроль территориального распределения обработки данных. Технологии геолокации преобразуют физическое пространство в более доступную для различных трансформаций среду (вычислено, измерено, проверено), это же утверждение актуально и для цифровой среды, цифрового сообщества, организованного в облачных вычислениях.

Понятие «геотегирования» представляет собой процесс определения, создания и инициализации набора объектов геолокации вычислительного устройства. Актуальным применением геотега является обеспечение соблюдения пограничного контроля на основе гео-тегов в концепции, называемой «гео-заслон». Концепция гео-заслона успешно применяется в мобильных компьютерах, в управлении цепочками поставок, транспортной логистике.

Приложения, поддерживающие гео-заслон, позволяют администратору устанавливать правила и применять их в автоматизированном режиме при изменении границ нахождения устройств, а также в отношении задач или областей данных с выдачей соответствующих предупреждений для дальнейшего расследования инцидентов

Согласно указанной концепции, при подключении к блоку управления клиент облачного провайдера осуществляет инициализацию меток и компонентов управления жизненным циклом принадлежащих ему данных, а также осуществляет доступ к конкретному физическому серверу для осуществления контроля целостности платформы и доверенного хранения геометок. На следующем этапе, используя средства проверки и аттестации (в прозрачном «сквозном» режиме), клиент допускается к взаимодействию с режимом выполнения виртуальной машины (через блок управления облаком и порталами, предоставленным провайдером и состоящим из системы контроля конфигураций и анализа информации, средств выполнения правил, средств управления рисками). Управление виртуальными службами осуществляется с помощью интерфейсов прикладного программирования (vCenter, OpenStack), что позволяет осуществлять необходимый контроль развертывания задач.

Информационная система, построенная с использованием технологий «облачных вычислений» (далее ИСОТ) состоит из множества различных аппаратно–программных средств, поддерживающих функционирование виртуальной среды. Использование разнообразного обеспечения, зачастую от разных производителей может повлечь не только сбои в работе виртуальной среды, но и порождает и провоцирует множество различных атак на неё. При этом процесс эволюции как программно-аппаратных средств, так и непосредственно информационной среды можно сравнить с биологической эволюцией: совместная коэволюция атакующих-защищающих, приводит к тому, что для обеспечения безопасности обработки информации облачной инфраструктуры недостаточно установки какого-либо одного средства защиты информации. Из-за повышения вероятного преодоления систем защиты при получении несанкционированного доступа к управлению виртуальной средой возрастает значимость построения ряда процессов обеспечения информационной безопасности (ИБ).

Важным условием для этого построения ИБ ИСОТ является определение места потенциального проведения атаки с целью её предотвращения, согласно представленному далее обзору, технология геометок перспективна для реализации механизма контроля географического перемещения данных. Подобно созданию периметра при освоении территорий Нового света геометки позволяют контролировать частную собственность в виртуальной среде.

Предлагается создание автоматизированной информационной системы для наблюдения и контроля размещения распределенной обработки данных. В основу системы предлагается онтологическое описание географического ландшафта вычислительной структуры, позволяющей классифицировать угрозы выхода за границу ландшафта, обеспечить требуемый контроль и предоставить удобный интерфейс на основе ГИС.

Облачные технологии не только изменили понятие «платформа», виртуализировав взаимоотношения операционной системы с оборудованием, но и остро поставили перед ИБ ИСОТ задачу по созданию «периметра», контролю точки входа пользователя, географическая привязка места входа является наиболее надежным методом аутентификации. Подтверждение подлинности удаленного пользователя по его местонахождению, является перспективным направлением аутентификации. Т.к. большинство устройств не обладает GPS-модулем, определение местоположения возможно по информации о местоположении серверов, соседних точек доступа GSM и WiFi связи, в зоне действия которых находится пользователь, через которые необязательно осуществляется подключение к сети интернет.

Саенко И.Б., Ганя С.С.
Россия, Санкт-Петербург,Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»

ТЕХНИЧЕСКИЕ ПРИНЦИПЫ И МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОРГАНИЗАЦИИ И РАЗВЕРТЫВАНИЮ РЕШЕНИЙ ПО АГРЕГАЦИИ, НОРМАЛИЗАЦИИ, АНАЛИЗУ И ВИЗУАЛИЗАЦИИ БОЛЬШИХ МАССИВОВ ГЕТЕРОГЕННЫХ ДАННЫХ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ В СЕТЯХ «ИНТЕРНЕТ ВЕЩЕЙ»

Процессы агрегации, нормализации, анализа и визуализации данных играют решающую роль при функционировании систем мониторинга сетей «Интернет вещей». От качества проведения этих процессов непосредственно зависит качество принимаемых решений по обеспечению безопасности сетей «Интернет вещей» и, следовательно, безопасность сетей и обрабатываемой в них информации в целом. В докладе рассматриваются аспекты практической реализации математических методов и алгоритмов, разработанных для выполнения процессов агрегации, нормализации, анализу и визуализации больших массивов гетерогенных данных для мониторинга безопасности в этих сетях.

Реализация процессов агрегации данных основывается на решении трех последовательно связанных задач. Первая задача заключается в определении последовательностей выполнения операторов потоковой обработки данных для вычисления мер центральной тенденции и экстремумов данных. Вторая задача осуществляет формирование схем распараллеливания операторов потоковой обработки. Третья подзадача выполняет привязку схем распараллеливания операторов потоковой обработки к узлам транспортной сети «Интернет вещей». В ней учитываются параметры входных потоков, линий связи и агрегаторов.

Методы и алгоритмы нормализации гетерогенных данных основаны на предварительном преобразовании неструктурированных и полуструктурированных данных к структурированному виде согласно разработанного подхода. Они обеспечивают рациональное сочетание двух подходов, связанных с максимальным и минимальным сохранением атрибутов на каждом этапе нормализации.

Методы и алгоритмы анализа больших массивов гетерогенных данных ориентированы на формирование схем потоковой обработки данных о событиях безопасности на основе применения разработанных правил преобразования SQL-запросов.

Такой подход позволяет, с одной стороны, обеспечить релевантность результатов потоковой обработки больших данных, соответствующую релевантности обработки SQL-запросов в централизованной базе данных системы мониторинга и управления безопасностью. С другой стороны, за счет использования операторов потоковой обработки, а также выше рассмотренных методов и алгоритмов, достигается требуемая оперативность обработки данных, соответствующая реальному масштабу времени, т.е. интенсивности входного потока данных. При этом процесс анализа данных в сети «Интернет вещей», охватывает этапы фильтрации данных, преобразования данных, выявления отношений между данными и обнаружении вредоносной, аномальной и некорректной активности как отдельных источников сети «Интернет вещей», так и их групп. Анализ данных основан на использовании правил, шаблонов и нейросетевых технологий.

Математические методы и алгоритмы визуализации гетерогенных данных в сетях «Интернет вещей» предназначены для представления результатов агрегации и анализа следующими способами: а) визуализация с использованием GIS-систем; б) визуализация с помощью диаграмм и графиков; в) инфографические методы визуализации; г) табличные методы визуализации; д) иерархические методы визуализации. При этом к методам и алгоритмам визуализации предъявляются следующие технические требования: а) кластеризация больших массивов данных; б) автоматическая классификация массивов данных; в) «ленивая» загрузка массивов данных при визуализации; г) детализация кластеризованных данных (Drill-down); д) переход между связанными данными; е) микширование данных (mesh-up).

В основе организации и развертыванию решений по агрегации, нормализации, анализу и визуализации больших массивов гетерогенных данных для мониторинга безопасности в сетях «Интернет вещей» лежит использование программно-инструментальной системы потоковой обработки данных. Система потоковой обработки данных выполняет обработку потоков данных путем выполнения над ними операций двух типов: а) без сохранения состояния; б) с сохранением состояния. Данные операции во-многом аналогичны операциям, которые выполняются над таблицами данных в реляционных базах данных. Основными операциями потоковой обработки данных являются операции Map, Filter и Union (первого типа), а также Aggregate и Join (второго типа). Примером системы потоковой обработки данных является система Spark Streaming.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (соглашение № 14.604.21.0147, уникальный идентификатор соглашения RFMEFI60414X0147).

Саенко И.Б., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Термин «информационное пространство» предполагает построение системы хранения и обработки информационных ресурсов на концепции «пространства данных», которая развивает известные концепции «базы данных» и «хранилища данных» и дополняет их новыми компонентами и свойствами. Информационное пространство 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 информационного пространства 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 информационного пространства является необходимость разработки моделей и методов для оценки эффективности ее функционирования. Специфика данных моделей и методов обусловлена тем, что система разграничения доступа в информационном пространстве, с одной стороны, должна обеспечивать сохранение значений функциональных показателей разграничения доступа, имеющихся у отдельных субъектов доступа (пользователей либо автоматизированных систем) до их вхождения в информационное пространство, а с другой – обеспечивать поддержание значений новых функциональных показателей, характеризующих эффективность доступа одних субъектов доступа к ресурсам других субъектов доступа.

При этом система разграничения доступа к ресурсам информационного пространства должна обеспечивать комплексирование различных моделей разграничения доступа (дискреционной, мандатной, ролевой и т.д.), присущих отдельным субъектам доступа, и возможность сохранения исходной модели разграничения доступа при выполнении операции проекции информационного пространства на отдельный субъект доступа. Операция проекции информационного пространства определяется как разновидность операции среза в многомерном гетерогенном пространстве по фиксированным значениям на различных измерениях, определяющих положение отдельного субъекта доступа.

Предлагаемые модели и методы оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства основываются на принципах имитационного моделирования попыток несанкционированного доступа, а также автоматической генерации объектов и полномочий доступа. В качестве показателей эффективности функционирования системы разграничения доступа используются значения количества ошибок первого и второго рода, совершаемых за заданный период модельного времени, а также рассчитываемая на их основе вероятность реализации несанкционированного доступа. В ходе автоматической генерации объектов и полномочий доступа учитываются заданные плотности распределения значений последних, а также общие количественные ограничения. Кроме того, в компоненте генерации используется различные алгоритмы поиска рациональных вариантов построения системы разграничения доступа.

В частности, одним из разновидностей реализованных алгоритмов являются генетические алгоритмы оптимизации схем разграничения доступа к информационным и коммуникационным ресурсам. Данные алгоритмы позволяют решать NP-полные задачи оптимизации, встречающиеся, например, при формировании ролевой модели доступа (Role-Based Access Control), структуры виртуальной локальной сети (Virtual Local Area Network), топологии сети каналов виртуальной частной сети (Virtual Private Network) и в других задачах.

На основе предложенных моделей и методов оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства разработан программно-инструментальный стенд, позволяющий генерировать различные варианты построения системы разграничения доступа и осуществлять оценку ее эффективности. В качестве одного из сценариев построения системы разграничения доступа рассматривалась схема построения виртуальных локальных подсетей, объединяющих удаленных пользователей информационного пространства. Помимо аналитической оценки различных вариантов построения системы разграничения доступа, программно-инструментальный стенд обеспечивает визуальное представление хода формирования подмножества наилучших решений, что позволяет администратору безопасности компьютерной сети выявлять «узкие места» формируемой системы разграничения доступа и повышает его уверенность в обоснованности принимаемых решений по обеспечению безопасности информации.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №1.5).

Тындыкарь Л.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

АСПЕКТЫ ПРИМЕНЕНИЯ SCADA-ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И КОМПЛЕКСОВ

Диспетчерское управление и сбор данных с помощью SCADA-систем (Supervisory Control And Data Acquisition) является основным и в настоящее время остается наиболее перспективным методом автоматизированного управления сложными динамическими системами (процессами) в жизненно важных и критичных с точки зрения безопасности и надежности областях, а также позволяет решить следующие задачи:

– обмен данными с «устройствами связи с объектом» (т.е. с промышленными контроллерами и платами ввода-вывода) в реальном времени через драйверы;
– логическое управление;
– обработка информации в реальном времени;
– отображение информации на экране монитора в удобной и понятной для пользователя форме;
– ведение базы данных реального времени с технологической информацией;
– аварийная сигнализация и управление тревожными сообщениями;
– подготовка и генерирование отчетов о ходе технологического процесса;
– осуществление сетевого взаимодействия между SCADA-системой и компьютером;
– обеспечение связи с внешними приложениями (системами управления базами данных, электронными таблицами, текстовыми процессорами и т.д.).

Перспективной разработкой становится создание систем, которые обеспечат диспетчеризацию и контроль (мониторинг) состояния сооружений и оборудования.

Главными целями создания таких автоматизированных информационно-управляющих систем являются:

– внедрение инновационных технологий управления объектами технологической инфраструктуры;
– предупреждение аварийных ситуаций, связанных с работой оборудования;
– повышение безопасности;
– снижение времени простоя в случае возникновения нештатных ситуаций;
– улучшение качества обслуживания оборудования.

Федорченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРАВИЛО-ОРИЕНТИРОВАННЫЙ МЕТОД КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ

В наше дни все больше внимания уделяется обеспечению безопасности информации как в государственном и промышленном секторах, так и в средних и малых организациях. Защищаемые объекты имеют различные уровни доступа, всевозможные варианты развертывания вычислительных сред и разнообразные топологии обеспечения сетевого взаимодействия. Задача обеспечения безопасности с помощью универсальных средств обнаружения и предотвращения атак усложняется за счет стремительного роста абонентов окружения и их разнообразия (изобилие встраиваемых устройств), использования облачных технологий и многократное увеличение обрабатываемой информации. Одним из классов средств, позволяющих обеспечивать безопасность систем любого уровня и набора устройств, являются SIEM-системы. Преимущество данных решений заключается в

гибкости применения и независимости от набора спецификаций и платформ для конечной защищаемой инфраструктуры.

Процесс корреляции информации и событий безопасности, который является основополагающим элементом применяемых механизмов обеспечения безопасности, решает задачи фильтрации и агрегации, выявления атаки, ее источника и цели.Также в данный процесс включены функции пред (пост) обработки информации в зависимости от конкретной реализации системы.

Правило-ориентированный метод корреляции относится к сигнатурным методам, являясь классическим и широко-распространенным не только в SIEM-системах, но и системах обнаружения вторжений, антивирусных решениях. В основе данного метода лежат правила, имеющих понятный системе анализа синтаксис и семантику. Собственно результирующим критерием в данном методе является правило, как самостоятельная оперативная единица (то есть операция может осуществиться за счет лишь одного правила).

Все правила для каждой операции обработки данных находятся в специально-отведенной таблице. При поступлении данных на вход в конкретную операцию, они проходят проверку на предусловие, а именно: соответствие определенному типу, наличие у заданных атрибутов определенных значений или принадлежность к определенному диапазону значений и т.д. Также правила можно разделять на простые и сложные. Например, простым правилом можно назвать такую запись в таблице, для положительного исхода которой (применения правила) достаточно выполнения одного предусловия.

В свою очередь, к сложным правилам относится набор из простых и сложных правил, связанных логическими операторами (И, ИЛИ, НЕ) и их комбинациями. Правила в таблице можно добавлять, удалять и изменять в процессе работы всей системы, поэтому данный метод относится к динамическим по характеру изменения результирующего критерия. Однако, ввиду сложности составления самих правил, по способу изменения данный метод принадлежит к изменяемым вручную, так как в основу правил входит качественный анализ данных, а не количественный.

Основным преимуществом описанного метода является отсутствие погрешностей при принятии решения, однако это не исключает ошибок, связанных с пересечением правил, например при удовлетворении предусловий сразу нескольких правил, с противоречивыми друг к другу результатами их выполнения. Для преодоления данной конфликтной ситуации в модулях, использующих данный метод, необходимо использование процедур проверки правил на наличие противоречий при изменении записей таблицы правил. К главному недостатку данного метода относится большая емкость правил и сложность их составления для наиболее рациональной обработки как с точки зрения достижения оптимальной точности анализа, так и минимизации затрачиваемых ресурсов на его выполнение.Не смотря на указанную сложность реализации процесса корреляции за счет правило-ориентированного метода, его применение не исключено ни из одной существующей SIEM-системы, однако данный метод используется преимущественно в комплексе со статистическими методами корреляции.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451).

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

ПОДХОД К ФОРМИРОВАНИЮ ПАТТЕРНОВ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Исходя из поставленной задачи 2015 года ежегодного конкурса VAST (The Visual Analytics Science and Technology), предлагается подход к формированию паттернов поведения пользователей в информационной системе. Данный конкурс предназначен для создания новых инновационных моделей визуализации, подходов обработки большого объема информации, решающих комплекс проблем, возникающих при работе с большими данными.

Начальным условием решаемой задачи является динамическая система, представляющая собой парк развлечений с посетителями, наборы данных о передвижении которых предоставили организаторы конкурса. Сами наборы состоят из записей, которые содержат следующие поля:

- дата,
- время,
- идентификатор пользователя,
- координата "x",
- координата "y".

Главной целью поставленной задачи является выявление аномального поведения людей в парке.Задача включает несколько подзадач:

- Охарактеризовать движение как групп, так и отдельных людей (далее пользователей) по всему парку (в информационной системе).

– Выявить связи между пользователями информационной системы, которые возникают с течением времени.

– Объединение решений подзадачи отдельных людей и подзадачи пользователей с выявленными связями.

Предлагаемый подход включает в себя формирование двух типов динамических графиков, позволяющих получить траекторию передвижения людей, а также граф связей, возникающих между ними. Предполагается, что есть возможность динамического построения графиков относительно определенного момента времени, тем самым обеспечивая детальное изучение поведения определенных пользователей.

Первый график описывает передвижение пользователей в системе декартовых координат, он позволит оценить человеческий фактор и выявить паттерны поведения относительно их перемещения. Следует отметить, что параллельно построению первого графика строиться граф контактов пользователей друг с другом. С помощью данного графа существует возможность получить статистику не только относительно всех пользователей, но и относительно группы или даже связи пользователей один к одному.

Сопоставляя графы между собой, появляется возможность выявить аномальную активность пользователей информационной системы, решая тем самым поставленную задачуформирования паттернов поведения пользователей в информационной системе.

Ханыков И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СОПОСТАВЛЕНИЕ ДВУХ МЕТОДОВ АВТОМАТИЧЕСКОЙ СЕГМЕНТАЦИИ

Компьютерное зрение применяется в различных областях народного хозяйства, индустрии, в военном деле и в научных исследованиях. Например, в медицине – для диагностики состояния пациента, в военном деле – для разведки и мониторинга обстановки, в промышленности – как средство контроля производства, в охранных системах – как средство наблюдения обстановки.

Востребованность систем компьютерного зрения подчеркивает значимость задачи выделения объектов на изображении – сегментации изображения. Существующие решения строятся по схеме выделения целевого объекта (текста, лиц, и пр.) по его априори заданным ключевым признакам. Каждое отдельное решение узконаправлено и ограниченно в возможностях распознавания объектов. Возникает актуальная задача разработки унифицированного инструмента сегментации, выполняющего сегментацию «вслепую» без априорной информации о содержании изображения.

В работе проведено сопоставление двух методов слепой сегментации изображения: метод адаптивной сегментации изображения по цвету и текстуре, и метод построения кусочно-постоянного приближения сегментированного изображения.

В методе адаптивной сегментации изображения по цвету и текстуре начальном этапе вычисление признаков выполняется раздельно. В качестве цветовых признаков используется компактное цветовое представление в терминах доминирующих цветов в векторном виде, которые могут быть получены рядом алгоритмов, Команицу-Мейера или адаптивным алгоритмом кластеризации. Области изображения и соответствующие им полученные вектора доминирующих признаков связываются по критерию оптимального расстояния цветовой композиции «OCCD». Вычисление критерия сводится к оптимизационной задаче поиска минимальной «стоимости» графа. В качестве текстурных признаков используются энергетические коэффициенты. Текстурные границы подчеркиваются, исключая плавные переходы. Затем осуществляется «сборка» текстурных сегментов одного типа. Затем начинается процесс последовательного объединения полученных сегментов. За промежуточной грубой сегментацией, получаемой путем наложения цветовых сегментов на выделенные текстурные области («раскраска» текстурных областей), следует этап получения конечной сегментации путем «коррекции» границ цветовых сегментов.

В основе модели метода построения кусочно-постоянного приближения сегментированного изображения лежат следующие положения. Изображение состоит из вложенных «объектов». Вложенный «объект» образуют усредненные по яркости (цвету) пиксели. При сегментации его формируют только смеженные пиксели. При кластеризации – несмежные сегменты. Образованное из таких объектов изображение называется кусочно-постоянным приближением. Качество разбиения и соответствующего приближения изображения численно оценивается по суммарной квадратичной ошибке. Во избежание высокой вычислительной сложности на выходе метода – последовательность иерархических квазиоптимальных приближений. Метод выполняется в три этапа. Сперва изображение разбивается на связные сегменты в модели Мамфорда-Шаха. Затем формируются суперпиксели в алгоритмах улучшения качества сегментации, которые потом кластеризуются производится по методе Уорда.

В результате сопоставления выявлены основные особенности каждого метода. Основное преимущество методов в том, что они относятся к классу методов автоматической сегментации.

Определенный интерес представляет исследование алгоритма построения карта доминирующих цветов для соответствующего ей изображения, в котором, во-первых, пространственная вариация цветов отсутствует, а, во-вторых, области усредненных яркостей соответствуют цветовым границам, которые могут не совпадать с границами воспринимаемых объектов на изображении. Аналогичные результаты получаются и в методе сегментации кусочно-постоянными приближениями. С этой точки зрения, в дальнейшем интерес заключается сопоставлении результатов алгоритма Команицу-Мейера с результатами модели Мамфорда-Шаха.

Харинов М.В., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛЬ КВАЗИОПТИМАЛЬНОЙ СЕГМЕНТАЦИИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

В настоящее время в области распознавания изображений особенно актуальной становится, так называемая, «проблема сегментации», или проблема автоматического выделения объектов, которая начинает формулироваться и решаться как наукоемкая инженерная задача.

При решении проблемы одной из главных задач является создание программно-алгоритмического обеспечения предварительной обработки цифровых изображений, с помощью которого достаточно квалифицированный программист сможет успешно решать задачи выделения на изображении конкретных объектов для их последующего распознавания.

Для создания требуемых программных средств необходимо:

– построить интуитивно понятную, наглядную модель изображения;

– в рамках модели определить понятие «объекта»;

– разработать и программно реализовать структуру данных, которая поддерживает скоростные операции с наглядно представляемыми «объектами» в доступном объеме оперативной памяти.

Многолетнее развитие идеи «адаптивной» иерархической сегментации в сочетании с идеей оптимизации разбиений изображения кусочно-постоянными приближениями, стандартным образом оцениваемыми по суммарной квадратичной ошибке аппроксимации изображения, привело к созданию подходящей, на наш взгляд, модели иерархической квазиоптимальной сегментации цифрового изображения.

Суть предложенной модели раскрывается пятью основными положениями:

1. Изображение состоит из изображений, которые задаются кусочно-постоянными приближениями изображения и именуются «объектами».

2. Объекты составляют бинарную иерархию.

3. Последовательность приближений представима в виде изображения, называемого «инвариантным представлением».

4. Любая тройка вложенных друг в друга изображений описывается выпуклой последовательностью значений суммарной квадратичной ошибки приближения от изображения.

5. Любая иерархическая последовательность приближений по определенному алгоритму преобразуется в последовательность приближений, описываемых выпуклой последовательностью значений суммарной квадратичной ошибки или среднеквадратичного отклонения приближения от изображения.

В первом положении утверждается, что изображение рассматривается как множество, состоящее из объектов той же природы. При этом термины «изображение», «объект», «кластер пикселей», в частности, «сегмент изображения», используются как синонимы, и при вычислениях обрабатываются по единым алгоритмам.

Благодаря второму положению в вычислениях удается обойти NP-трудную задачу получения оптимальных приближений изображения, которая заменяется полиномиально сложной задачей аппроксимации неиерархической последовательности оптимальных разбиений посредством иерархической последовательности квазиоптимальных приближений изображения. Тогда очевидно, что задача аппроксимации решается, в этом случае, не однозначно.

Согласно третьему положению иерархическую последовательность приближений можно задать как новое изображение, которое называется «инвариантным представлением», так как не меняется при определенной модификации исходного изображения, например, линейном преобразовании по яркости и др.

Четвертое положение устанавливает закон, согласно которому квазиоптимальные приближения описываются выпуклой зависимостью суммарной квадратичной ошибки, как и оптимальные.

Согласно пятому положению любая иерархическая последовательность приближений преобразуется в последовательность квазиоптимальных приближений, которые:

– ограничены по числу сегментов;

– близки к изображению по суммарной квадратичной ошибке;

– в зависимости от числа кластеров описываются выпуклой последовательностью значений суммарной квадратичной ошибки.

Таким образом, изображение описывается семейством переплетающихся выпуклых кривых и массивом инвариантных представлений, порождающих «инвариантное пространство», которое отличается от традиционного признакового пространства тем, что в качестве признака учитывает единственную среднюю яркость по-разному усредняемых пикселей.

В докладе демонстрируются преимущества модели иерархической квазиоптимальной сегментации в задаче улучшения сегментации, полученной по различным алгоритмам, а также обсуждается наилучшая область применения модели.

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

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И АЛГОРИТМЫ МОДЕЛИРОВАНИЯ АТАК И ВЫРАБОТКИ КОНТРМЕР В РЕЖИМЕ, БЛИЗКОМ К РЕАЛЬНОМУ ВРЕМЕНИ

Одной из фундаментальных научных проблем является разработка методологических основ обеспечения безопасности информации в информационно-телекоммуникационных системах. В настоящее время данные системы используются во всех областях от повседневной жизни, до управления критически важными инфраструктурами, и поэтому решение этой проблемы является одной из приоритетных задач, решаемых органами государственного, регионального и местного управления во всех развитых государствах мира.

Целью данного исследования является повышение уровня защищенности информационно-телекоммуникационных систем за счет разработки новых математических моделей, методик и алгоритмов анализа защищенности, моделирования атак и выработки контрмер в режиме близком к реальному времени.

Предполагается, что данная цель будет достигнута путем достижения следующих задач:

1. Разработка математических моделей и алгоритмов моделирования атак и выработки контрмер для защиты информации в информационно-телекоммуникационных системах на основе создания и применения средств аналитического моделирования и проактивного мониторинга.
2. Оптимизация процесса аналитического моделирования информационно-телекоммуникационной системы и ее системы защиты в условиях проведения атак в режиме близком к реальному времени.

Таким образом, обобщенной задачей данного исследования является разработка новых математических моделей и алгоритмов моделирования атак и выработки контрмер, которые могли бы использоваться в условиях больших объемов исходных данных и производить анализ системы защиты в условиях проводящихся атак в режиме близком к реальному времени, и, как следствие, рекомендовать оператору способы изменения политики безопасности системы защиты за ограниченное время.

Таким образом, система, основанная на результатах данного исследования, должна учитывать события безопасности, происходящие в реальном времени и адаптировать политику безопасности информационно-телекоммуникационной системы таким образом, чтобы максимально снизить возможные последствия проводящейся атаки.

С помощью реализации разрабатываемых моделей и алгоритмов, предполагается достичь значительного повышения уровня защищенности информационно-телекоммуникационных систем, обеспечить возможность манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности.

Система защиты информации, основанная на предложенном подходе должна обладать способностью успешно решать следующие задачи: получение информации о текущем состоянии защищенности информационно-телекоммуникационной системы и ее компонентов; проведение обоснованного анализа и управление рисками безопасности защищаемой информационно-телекоммуникационной системы (в том числе своевременное устранение или снижение рисков безопасности); обнаружение несоответствия реального уровня защищенности важных ресурсов требуемому уровню, определяемому внутренними политиками безопасности, и приведение их в соответствие друг с другом; принятие эффективных решений по защите информации.

Использование разрабатываемых математических моделей и алгоритмов моделирования атак и выработки контрмер позволит повысить уровень информационной безопасности за счет постоянного отслеживания текущих показателей защищенности в режиме, близком к реальному времени. Кроме того, предлагаемый подход позволит производить предварительную оценку влияния предлагаемых оператором контрмер на защищенность информационно-телекоммуникационной системы что позволит повысить качество принимаемых решений.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451).

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

ПРОТОКОЛЫ ПОРОГОВОГО ОТРИЦАЕМОГО ШИФРОВАНИЯ

Пороговые криптосхемы предполагают участие некоторого коллективного органа, включающий M больше одного пользователей. При этом для корректного функционирования пороговых криптосхем требуется участие не менее T, где T меньше M пользователей, входящих в штат коллективного органа. Участие последнего в криптографических протоколах обеспечивает повышение уровня информационной безопасности к атакам с участием внутренних нарушителей, а условие T меньше M – достаточную гибкость при практическом использовании пороговых криптосхем. Известны пороговые схемы разделения секрета, пороговые схемы групповой цифровой подписи, пороговые протоколы аутентификации и пороговые протоколы открытого шифрования. В настоящем сообщении предлагается новый тип пороговых криптосхем -- пороговые протоколы отрицаемого шифрования.

Отрицаемое шифрование предназначено для обеспечения защиты информации к атакам с принуждением отправителя и/или получателя раскрыть секретный ключ, использованный при шифровании. Известны протоколы отрицаемого шифрования с использованием шифрования по разделяемому секретному ключу и с использованием шифрования по открытому ключу получателя сообщения. Пороговые протоколы отрицаемого шифрования могут применяться для обеспечения возможности раскрытия секретного сообщения некоторым коллективом. Отправитель сообщения направляет шифртекст, содержащий сообщение, в контейнер, доступный n доверенным лицам.

Для обеспечения возможности расшифрования сообщения усилиями T доверенных лиц (T меньше M) отправитель отправляет каждому из n доверенных лиц долю ключа шифрования. При объединении t долей имеется возможность восстановить секретный ключ и восстановить секретное сообщение из криптограммы. При наличии менее, чем T долей, восстановление секретного ключа не менее сложно, чем его восстановлении без знания какой-либо доли.

При выполнении атакующим принуждающей атаки отправитель предоставляет фиктивный ключ, а получатели – фиктивные доли секрета, по которым восстанавливается фиктивный ключ, такой же как и предоставленный отправителем. Используя фиктивный ключ атакующий расшифровывает шифртекст (который он перехватил в процессе передачи шифртекста по открытому каналу), в результате чего восстанавливается осмысленное фиктивное сообщение. Наличие фиктивного ключа не облегчает атакующему вычисление секретного сообщения.

Разработаны пороговые схемы отрицаемого шифрования двух типов, отличающиеся использованием открытого или разделяемого секретного ключа. Предложенные протоколы удовлетворяют требованию неотличимости шифртекста, поученного в процессе отрицаемого шифрования, от шифртекста, полученного в процессе вероятностного шифрования.

Обсуждается использование трудности задачи факторизации и задачи дискретного логарифмирования для построения предлагаемых пороговых протоколов отрицаемого шифрования.

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ОЦЕНКА РИСКОВ УТЕЧКИ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИИ ПРИ ЭКСПОРТЕ ПРОДУКЦИИ ДВОЙНОГО НАЗНАЧЕНИЯ

Естественное для предприятий и организаций экспортёров стремление выйти на мировые рынки с высокотехнологичной продукцией наряду с безусловными преимуществами, очевидно, порождает риски передачи разного рода информации, утечка которой может оказаться недопустимой, если не ограничиваться исключительно краткосрочными экономическими соображениями. В долгосрочной перспективе даже в чисто экономическом смысле такого рода утечки грозят потерей, по крайней мере, приоритета и конкурентных преимуществ, не говоря о потенциальном ущербе для государственных интересов.

В то же время инновационная деятельность поощряется государством, причём предпочтение отдаётся малым формам предпринимательства, однако особенно рискованной в указанном смысле может быть внешнеэкономическая деятельность именно молодых компаний с малой капитализацией. Во-первых, глубина видения бизнеса во времени имеют прямую зависимость от неё, а, во-вторых, общее снижение культуры производства и квалификации кадров, произошедшее за постсоветский период в сочетании с отсутствием достаточного опыта ведения дел с зарубежными партнёрами создают дополнительные риски.

В первую очередь приведённые аргументы можно отнести к отечественной ИТ-отрасли, значительное количество представителей которой привыкли ориентироваться на западный рынок

(особо отметим тех, что работают на территориях недавно вошедших в юрисдикцию РФ) и в среде которых, кроме того, характерны космополитические настроения.

Однако не следует думать, что такого рода риски отсутствуют у крупных производителей высокотехнологичной продукции, которая в настоящее время в большинстве случаев может рассматриваться как продукция двойного назначения. Борьба за крупные проекты и демонстрация конкурентных преимуществ может снизить порог контроля допустимости раскрытия информации. Не надо забывать при этом и о скрытых каналах утечки информации, которые возникают не явным образом при интенсивном и не всегда должным образом контролируемом информационном обмене.

Нормативные и административные инструменты экспортного контроля, безусловно, важны, необходимы и определённым образом препятствуют реализации рисков, однако, как и всякий регламент, не являющийся тотально запретительным, они не способны в полной мере, учитывая названные факторы, предотвратить нежелательные утечки.

Таким образом, есть объективная потребность усилить возможности контроля, но не за счёт ужесточения регламентов, а средствами более содержательного и конкретного анализа рисков. На наш взгляд такие возможности способна предоставить разрабатываемая нами автоматизированная система риск-анализа, в рамках одного из направлений её развития - создания так называемых предметно-ориентированных риск-моделей, позволяющая насколько возможно полно учесть имеющийся опыт и экспертные знания в разнородном виде и сложное взаимодействие многочисленных факторов риска, с получением количественных оценок стохастического профиля риска.

Тогда, разработав такую риск-модель утечки критически важной информации при экспорте продукции двойного назначения, с одной стороны, можно будет её использовать для самоконтроля ответственных производителей, а с другой – для совершенствования, уточнения и оценки эффективности административных процедур.

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СИМПТОМЫ, СИНДРОМЫ И УГРОЗЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Употребление термина «симптом» не характерно для сферы информационной безопасности и вообще в технике. Возможно, вместо него привычнее было бы использовать общетехнический термин индикатор или какой-либо подобный. Однако первый вариант нам представляется более точным, исходя из цели сообщения. Она состоит в том, чтобы, если не противопоставить, то подчеркнуть принципиальное отличие собственно угроз, то есть событий, действий, прямо или косвенно приводящих к нарушению, ущербу для безопасности, и их признаков (симптомов), то есть неких проявлений, особенностей поведения контролируемой системы, может быть, связанных с реализацией угроз, а, может быть и вполне безобидных или, во всяком случае, не опасных по своей сути. Например, так называемая «подозрительная активность», которую не трудно определить во входящем трафике может свидетельствовать как о попытке проникновения, так и объясняться естественными колебаниями активности или маскировкой совсем других, действительно угрожающих действий, то есть её следует рассматривать лишь как симптом возможной «болезни».

Более того, вполне уместным и полезным для употребления может быть и другой медицинский термин «синдром», поскольку признаки нарушения безопасности в информационных системах редко проявляются одиночно, а чаще в некоторой связанной совокупности.

Во всяком случае, любая более или менее сложная атака всегда имеет множество проявлений симптоматического характера, на которые можно не обратить внимание, если контролировать исключительно события-угрозы. С другой стороны, если симптомы будут рассматриваться как угрозы, то неизбежно неадекватное реагирование системы защиты. Поэтому важно, как и в медицине, стремиться лечить не симптомы, а болезнь.

Таким образом, целенаправленное определение симптомов угроз и их связных комплексов может дать дополнительные возможности для индикации нарушений безопасности и сокращения ошибок ложного реагирования на угрозы.

Для анализа симптоматики нарушения безопасности предлагается использовать подход, реализованный нами в разработанной автоматизированной системе риск-анализа. Основой применённой в ней методики является построение структурно связной и причинно-обусловленной модели угроз, понимаемых в указанном выше узком смысле. Расширение модели не потребует изменения методической основы и существенной модификации алгоритмов. Тогда, выявив кроме угроз сопутствующие им события-симптомы, некоторые из которых, возможно и неочевидным образом окажутся связаны как синдром, получив оценки их значимости в системе взаимодействия всех факторов риска, можно будет выработать новый взгляд на построение систем защиты информации.

Шкарбан А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

МОНИТОРИНГОВЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ НА БАЗЕ МУЛЬТИАГЕНТНОГО ПОДХОДА

В статье рассмотрен вариант развития систем безопасности. Среди примеров, иллюстрирующих необходимость качественного развития систем данного класса – не так давно обнаруженное лабораторией Касперского «крупнейшее банковское ограбление», когда в результате хакерской атаки пострадали более ста банков и других финансовых учреждений в 30 странах, или, например, несанкционированное срабатывание системы пожаротушения 8.11.2008г. на подводной лодке К-152 «Нерпа», повлекшее смерть 20-ти человек, а также взрыв нефтяной платформы DeepwaterHorizon в Мексиканскомзаливе. По мнению автора, этих и многих других инцидентов можно было избежать, или, как минимум, существенно сократить затраты от последствий, если применить новый подход к построению систем безопасности.

В ходе функционирования любой сложной производственной или информационно-вычислительной системы возникают инциденты безопасности. Исследование таких ситуаций показало, что в подобных системах существуют уязвимые (проблемные) зоны:

– неадекватность ответных мер в силу неспособности адекватной оценки в условиях неопределенности;

– влияние человеческого фактора, включающее участие людей, принимающих решения, или выступающих в роли исполнительных элементов;

– долгое время реакции систем, работающих на «жестких» сценариях и обладающих ограниченным набором стандартных датчиков данных, на нестандартные ситуации.

Улучшить системы безопасности предлагается с помощью мультиагентногоинтеллектуального подхода. Ниже перечислены преимущества данного подхода, позволяющие повысить эффективность систем безопасности:

1. Интеллектуальная обработка инцидента позволит более корректно распознать и классифицировать инцидент, избежать ложных срабатываний и применения неадекватных мер, а также избежать отсутствия срабатываний по причине отсутствия правил для конкретной сложившейся ситуации.

2. «Роевое поведение» агентов позволит более эффективно ликвидировать инцидент безопасности, так как агенты смогут напрямую взаимодействовать между собой и приходить к консенсусу.

3. Децентрализованное поведение агентов обеспечит стабилизацию работы системы и ее независимость от воздействия на «центральное звено».

Человек исключен из контура не полностью. Если в случае поиска решения, рой агентов решает, что сложившаяся ситуация (по значению показателей) слишком далека (на заданную величину) от описанной в правилах, рой выбирает наиболее близкие решения и производит эскалацию с предложением наиболее близких вариантов. Вариант эскалации по причине выхода за сроки, предусмотренные в SLA, предусмотрен как дань передовым практикам, но видится маловероятнымв силу гораздо более высокой скорости обработки данных программными агентами, нежели оператором в лице человека. Предпринимаемые системой шаги непрерывно регистрируются.

Результатом данного исследования является концептуальная архитектура и схема процесса для типовой системы управления инцидентами безопасности на базе мультиагентных технологий, которая дополняет классический контур управления понятиями программного (а в некоторых случаях и аппаратного) интеллектуального агента, интеллектуальной обработки события, генерации решения на основе консенсуса и самообучения системы.

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

ПОСТРОЕНИЕ МОДЕЛИ БЕЗОПАСНОЙ БИОТОПОЛОГИИ ДВИГАТЕЛЬНОЙ НАГРУЗКИ

Решается задача установления безопасной биотопологии двигательной нагрузки человека в рамках технологии построения модели выбора допустимой дозированной нагрузки для решения задач оздоровления человека. Предполагается наличие описания физического состояния биообъекта в параметрической полноте, достаточной для определения сценария двигательной нагрузки. Параметрическое описание содержит сведения о запретах, ограничениях и рекомендациях для конкретного биообъекта. Безопасный сценарий опирается на запреты и ограничения, выделенные в общей, групповой и персонифицированной среде допустимой нагрузки. Общий раздел содержит общие физиологические и анатомические ограничения; персонифицированный раздел - присущие конкретному человеку; групповой раздел содержит групповые множества, объединяемые по условиям задач сценариев оздоровления человека и человека в группе. Введены понятия разрешения / запрета на проведение движений с учётом степени строгости недопущения нагрузки: предельный запрет

исключает все виды нагрузки и трафику в биотопологии нагрузки, ограничения регулируют степень допустимости нагрузки и её трафика.

Информационная база эталонных трафаретов содержит базовый анатомический и физиологический материал для построения модели выбора допустимой дозированной нагрузки. Путём поэтапного введения / снятия ограничений на базовые модели выстраиваются сценарии двигательной нагрузки и модели безопасной биотопологии двигательной нагрузки. Исходной информацией для ограничений являются биокарты и индивидуальные модели с персональной информацией о человеке - физиологическое состояние объекта с такой параметрической обработкой информации, которая пригодна для построения и обработки моделей, а также фиксации начального состояния, динамики изменений, карты контроля промежуточного и финального состояние объекта.

Модели нагрузки строятся под определенную мотивацию задачи оздоровления от поддержания физического состояния человека до внесения изменений в его состояние. Под потребительскую мотивацию выстраиваются сценарии для решения желаемой или предписанной задачи оздоровления. В модели нагрузки по некоторому набору критериев формируются рабочие топологии модели, которые проверяются на степень нагрузочности и безопасность с точки зрения потребительской мотивации, анатомической и физиологической допустимости.

Необходимо построить возможные топологии решения задачи по предписанному сценарию, выбрать из них предпочтительные по некоторым критериям, установить их пригодность для достижения предписанного или желаемого результата. В разделе групповой пригодности содержатся групповые множества для сценариев оздоровления человека в группе. На основе модели биотопологии двигательной нагрузки и информационного описания биообъекта разрабатывается методология проведения мероприятий оздоровления и применяемых методик и процедур. Модель безопасной биотопологии двигательной нагрузки, упрощённо говоря, будет выглядеть усечённым вариантом эталонных трафаретов с базовым анатомическим и физиологическим наполнением, в котором исключены зоны ограничений, запретов и недопущений нагрузки. Вместе с тем характеристики разрешения / запрета и установления интенсивности нагрузки имеют плавающие границы а нацелены не только на отсекание объективных, возможных и потенциальных ограничений, но и в поиске вариантов снятия и ослабления запретов и ограничений как для случаев чрезмерных ограничений, так и в ходе положительной динамики в результате реализации намеченных мероприятий оздоровления и применяемых методик и процедур.

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

МЕТОДИКА БЕЗОПАСНОГО ЗОНИРОВАНИЯ ДЛЯ МОДЕЛИ ДВИГАТЕЛЬНОЙ НАГРУЗКИ

Рассматривается методика построения биотопологии модели для выбора допустимой дозированной нагрузки при решении задач оздоровления человека. Предполагается наличие описания физического состояния биообъекта в подготовленной параметрической полноте, достаточной для определения сценария двигательной нагрузки. Параметрическое описание содержит сведения о запретах, ограничениях и рекомендациях для конкретного биообъекта. В терминах модели вводятся понятия линий, пятен и зон нагрузки с характеристиками разрешения / запрета на проведение движений - по линиям, удержания интенсивности нагрузки - в зоне и недопущении нагрузки - в пятне (в строгом недопущении - с запретом на использование линий пятна). Зоны и пятна могут быть локальными, сводными, интегральными в зависимости от симптоматики их объединения. Разбиение на области, зоны и пятна вводит понятие безопасного зонирования при построении модели двигательной нагрузки.

Исходные строгие модели обладают эталонными трафаретами, с анатомическими признаками: по пятнам - с физиологическим наполнением, по линиям - с трафиками проводимости систем и частей тела человека, с зонами - потенциальные запреты и ограничения при переходе к частным моделям. Индивидуальные модели и биокарты содержат персональную информацию о физиологическом состоянии объекта, по которым строгие модели персонифицируются в трех аспектах - линии, пятна, зоны, фиксируется начальное состояние, динамика изменений, карты промежуточного и финального контроля. Расположение и качественное состояние пятен и зон отражает наличие разрешений / ограничений для двигательной активности биообъекта и степени интенсивности и предпочтительности линий. Модель нагрузки строится под определенный сценарий, мотивированный конкретной целью нагрузки - решение предписанной или желаемой задачи оздоровления от поддержания состояния до его коррекции.

Наибольший интерес представляет построение топологий биомодели для реализации решаемой задачи, когда требуется определить, выбрать и установить зоны нагрузки в их связности. Необходимо построить возможные топологии решения задачи по предписанному сценарию, выбрать из них предпочтительные по некоторым критериям, установить рабочую топологию модели для достижения предписанного или желаемого результата. Рабочим материалом для реализации

программы оздоровления являются схемы и протоколы в терминологии применяемых методик и процедур. Степень их детализации может различаться в широком диапазоне и напрямую не обязательно терминологически связана с механизмами построения модели, но схожесть информационного описания биообъекта, задачи оздоровления, методологии проведения мероприятий оздоровления и применяемых методик и процедур обеспечивают терминологическую основу, позволяющую контролировать как конструкторский, так и пользовательский раздел представления модели. В связи с этим единая терминология информационной поддержки всех циклов и этапов позволяет проследить именно методологию процесса построения биомодели, состав исходных строгих моделей и применяемых трафаретов, параметрическое описание объекта, мотивацию назначений пятен и зон, инициацию и нагрузочность линий. В этом случае направление исследования по безопасному зонированию для модели двигательной нагрузки понятны и обоснованы на конструкторском и пользовательском уровне применения модели.

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

ИЗОБРАЗИТЕЛЬНАЯ КИБЕРНЕТИКА. СИСТЕМНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ ТЕХНОЛОГИЧЕСКОЙ ДИСЦИПЛИНЫ ДИЗАЙН

Начертательная геометрия это – начертательные технологии геометрии. Дизайн в переводе с английского означает проектирование, конструирование, это – тоже технологии. Черчение, проектирование, это – технологические процессы по построению художественно-графического продукта, например: проектирование эстетического облика зданий или промышленных изделий. Это – та же информатика, с частичным, может быть, математическим расчетом, а порой и вовсе без него.

Дисциплина это – самостоятельная отрасль какой-либо науки, в которой есть порядок, последовательность.

Известно, что у всякой научной дисциплины должны быть теория и методика, направленные на практическое осуществление результата, причем теория дисциплины должна предшествовать методике и практике. Теория здесь – Кибернетика, а методики описывают технологические приемы, которые применяются в Начертательной геометрии и дизайне и т.д.

Сегодня появились названия "дисциплины": "Пропедевтика дизайна", " Пропедевтика", "Пропедевтика и критика", и т.д.

Приводит в сомнение образование названий и предложений со словом Пропедевтика. Пропедевтика – слово греческое, оно означает: обучаю предварительно, имеется в виду использование незначительного объема информации (основы), это – количественная величина информации, а не качественная. Она означает – введение, краткое освещение какой – либо теории, сокращенное изложение, направленное на подготовку мышления к логическому рассуждению. К слову сказать, увертюра к опере это еще не сама опера. Или, предисловие, это еще не книга.

После слова Пропедевтика, обязательно, должно стоять название дисциплины, введением в которую она является.

Примеры неправильного употребления:

Пример 1. Г.М. Гусейнов. Пропедевтика (Основы композиции). Учебно-методическое пособие…

Пример 2. Пропедевтика (Основы конструирования в дизайне)…

Пример 3. Программа дисциплины "Пропедевтика" для направления 072500.62, профиль "WEB" – дизайн (интернет)

"Пропедевтика" – не может быть дисциплиной, это – вводный курс, введение, основы какой-либо науки. Это – часть структуры текста, определенным образом организованная. А тексты могут быть о психологии, о детских болезнях, о геометрии,…

Пример 4.Название кандидатской диссертации: "Пропедевтика как универсальное средство и основа в системе художественного проектирования" и т.д.

Художественно-графические технологии должны быть, наконец, сведены в единую, стройную,логически обоснованную систему, описывающую производственные процессы на основе науки об управлении и связи.

И, может - быть, Санкт - Петербургский государственный университет технологии и дизайна, именовать "Изобразительной кибернетики"?

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Аванесов М.Ю.
Россия, Санкт-Петербург, ЗАО «Институт Телекоммуникаций»

УПРАВЛЕНИЕ ПОТОКАМИ ДАННЫХ В МОБИЛЬНЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ ПОВЫШЕННОЙ ЖИВУЧЕСТИ

Решение задачи повышения живучести инфокоммуникационной сети (ИС) в условиях широкого применения мобильной составляющей, обусловливающей динамическое изменение ее топологии, является одним из основных факторов, определяющих эффективность функционирования ИС. В настоящее время в условиях повышенных требований к живучести ИС широкое применение находят децентрализованные беспроводные сети, построенные по технологии ячеистых сетей (mesh-сети), в которых любой узел беспроводной сети может выступать как конечным потребителем информации, так и промежуточным узлом, через который ведется ретрансляция. В mesh-сетях наиболее эффективным является применение одного из двух методов управления потоками данных: зондовый метод и поисково-волновой метод. Алгоритмы, реализованные на основе зондового метода, являются проактивными и обеспечивают построение и постоянное поддержание актуальности плана распределения потоков данных в сети. Алгоритмы, реализованные на основе поисково-волновых методов, являются реактивными и осуществляют поиск маршрута только при наличии информации для передачи. Выбор метода управления потоками данных производится в зависимости от условий и особенностей применения средств связи. В случае если условия применения средств связи позволяют поддерживать непрерывный обмен данными и не накладывают ограничений по выходу в эфир средств связи, целесообразно применять зондовый метод управления потоками данных. Суть метода заключается в следующем: любой узел сети в произвольный момент времени рассылает по всем направлениям короткое сообщение – зонд. Узлы, принявшие зонд, анализируют информацию, содержащуюся в нем, и рассылают зонд по всем направлениям. Организовывается лавинное распространение зондов. Специальные механизмы селекции зондов не позволяют распространяться зондам, несущим избыточную информацию. В минимально короткое время зонды проходят через каждый узел сети, формируя на каждом узле полную матрицу маршрутов. Одновременное зондирование с нескольких узлов (так называемое перекрестное зондирование) позволяет обеспечить равномерное заполнение матриц маршрутов на всех узлах и быструю реакцию сети на изменение ее топологии.

Основным недостатком, присущим практически всем проактивным алгоритмам маршрутизации, является существенная нагрузка на сеть служебной информацией. При этом зависимость между объемом служебного трафика и размерами сети носит экспоненциальный характер. Это обуславливает ограниченность применения данных алгоритмов в больших сетях (более 100 узлов

Применение реактивных алгоритмов поиска кратчайших маршрутов, основанных на поисково-волновом методе, позволяет избавиться от постоянной нагрузки на сеть служебной информации, однако вносят существенную задержку при передаче полезного трафика. При использовании реактивных алгоритмов на узлах связи не хранится постоянно таблица маршрутизации, а при необходимости передачи информации осуществляют поиск маршрута волновым методом следующим образом: узел, обладающий информацией, требующей передачи, но не имеющий маршрута к конечному узлу, рассылает поисковый запрос, содержащий адрес конечного узла, по всем исходящим направлениям. Каждый узел, принявший поисковый запрос, проверяет, является ли конечным узлом. В случае если адрес конечного узла не совпадает с собственным адресом, узел дописывает в поисковый запрос собственный адрес и рассылает запрос далее по всем исходящим направлениям. Если адрес конечного узла совпадает с собственным адресом, то в обратном направлении направляется подтверждении об отыскании маршрута, при этом поисковый запрос уже содержит в себе кратчайший маршрут, по которому и отправляется подтверждение. Любой узел, оказавшийся промежуточным в цепи, сохраняет данные о проложенном через него маршруте. В случае выхода из строя канала связи, задействованного в маршруте, начальном узлу в маршруте отправляется сообщение о прекращении его действия, и начальный узел повторяет процедуру поиска кратчайшего маршрута.

В целом, использование проактивного алгоритма позволяет добиться сокращения до трех раз времени восстановления процесса передачи полезной информации в случае обрыва канала связи. При этом вне зависимости от структуры и связности сети гарантируется, что время восстановления не превысит времени восстановления при использовании реактивного алгоритма.

Таким образом, выбор методов управления потоками данных в мобильных ИС напрямую зависит от ограничений, связанных с возможностью непрерывной передачи данных каждым узлом, и от приоритетности требований, предъявляемых к живучести, оперативности и пропускной способности ИС.

Бабаджанян Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

НОВЫЕ АЛГОРИТМЫ ДЛЯ ТЕХНОЛОГИИ МНОГОУРОВНЕВОГО ШИФРОВАНИЯ

Технология многоуровневого шифрования нашла применение в средствах защиты информации (СЗИ), обрабатываемой в компьютерных системах, которые ориентированы на массовое применение (системы СПЕКТР-Z, СПЕКТР-М, Щит РЖД, системы семейства Аура). Данная технология предполагает исполь зование программно-ориентированных алгоритмов шифрования различного типа, в частности алгоритмов дискового шифрования: с большим размером входного блока, алгоритмов файлового шифрования и др. Дальнейшее совершенствование СЗИ, в которых используется технология многоуровневого шифрования, связано с применением отрицаемого шифрования, позволяющего реализовать новые механизмы защиты информации, и с разработкой алгоритмов дискового шифрования, обладающих более высокой производительностью. Решению последних двух задач были посвящены исследования, результаты которых представляются в данном сообщении.

Известные алгоритмы дискового шифрования, основанные на выборке подключей в зависимости от входных данных, ориентированы на использовании 2-разрядных микропроцессоров, тогда как на практике расширяется применение 64-разрядных процессоров. Для последнего случая предложен способ повышения производительности алгоритмов дискового шифрования путем уменьшения числа обращений к ключевому массиву с трех до одного. При этом переход от преобразования 32-разрядных слов к 64-разрядным дает дополнительное увеличение производительности в два раза. Уменьшение числа выборок достигнуто за счет применения операции умножения при формировании адреса выбираемого подключа. Уникальность последовательности подключей для текущего преобразуемого блока данных достигается посредством использования 64-битовой переменной, при формировании значения которой выполняется умножение ее предыдущего значения на значение текущего преобразуемого 64-битового слова входных данных.

Для встраивания защитных механизмов типа криптографических обманных ловушек в комплексные программные СЗИ предложено использование алгоритмов отрицаемого шифрования с разделямым секретным ключом, удовлетворяющих критерию вычислительной неотличимости по выходному шифртексту от алгоритмов вероятностного шифрования. Представляет интерес использование в СЗИ отрицаемого шифрования для выполнения криптографического преобразования 1) загрузчика операционной системы, 2) файлов и 3) жесткого диска. Для противодействия атакам, связанным с измерением времени расшифрования файлов к разрабатываемым алгоритмам, было предъявлено требование одинаковости всех операций процедуры расшифрования по секретному и фиктивному ключам. Для всех перечисленных типов ОШ были предложены программные алгоритмы ОШ, удовлетворяющие требованиям вычислительной неотличимости от вероятностного шифрования и независимости процедуры шифрования от ключа и обладающие достаточно высокой скоростью шифрования.

Рассмотрены варианты реализации программных алгоритмов ОШ для случаев использования 32-разрядных и 64-разрядных микропроцессоров. В основу алгоритмов положен предложенный недавно достаточно универсальный механизм формирования промежуточных шифртекстов, объединяемых в единый выходной шифртекст, представляющий собой решение систем линейных сравнений или линейных уравнений. Разработанные алгоритмы ОШ расширяют известный в литературе арсенал средств ОШ, включающий в себя алгебраические, коммутативные, блочные и поточные шифры.

Для случая шифрования на файловом уровне предложено комбинирование ОШ с алгоритмами сжатия данных, за счет чего может быть обеспечено уменьшение объема используемой памяти для хранения файловых данных. Также представляет интерес использование предварительного сжатия информации, содержащейся в отдельных передаваемых по открытым каналам сообщений, для которых требуется обеспечить защиту к атакам с принуждением отправителя и/или получателя к раскрытию ключа шифрования.

Белоусов А.С., Ныркov А.П.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ МЕТОДАМИ ВИРТУАЛЬНОГО СЕГМЕНТИРОВАНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Одними из возможных мест уязвимости информационной системы являются сети передачи данных этой системы. Сети передачи данных построены с использованием различных сетевых устройств, соединяющих их кабельных трасс и аппаратных средств беспроводного доступа. Чаще всего из-за экономической и производственной выгоды, сети физически коммутируются в один физический сегмент, тем самым возникает угроза безопасности сразу всей информационной системе.

Одним из методов обеспечения защищенности сетевой инфраструктуры информационной системы является разделение физической сети на виртуальные локальные вычислительные сети (VLAN). Виртуальная сеть представляет собой программно-обособленный сегмент основной сети. Взаимодействие устройств различных виртуальных сетей происходит по заранее определенным правилам. Такие правила могут полностью запрещать взаимодействие или разрешать его частично.

Существуют четыре технологии создания VLAN:

– порт коммутатора приписывается к определённой VLAN и физический коммутатор делится на необходимое количество различных логических портов;
– отнесение устройств к определённым логическим сетям на основе их MAC-адреса;
– объединение устройств в виртуальные сети по сетевым протоколам;
– многоадресная группировка.

В соответствии со стандартом IEEE 802.lQ, каждой виртуальной сети присваивается номер, который передается в специальном 12-битном поле кадра TAG. Максимально возможное число виртуальных сетей в составе одного сегмента физической сети составляет 4096. При обработке пакетов данных коммутирующее оборудование, передает информацию в виртуальную сеть, которой принадлежит этот пакет, исключая остальной сегмент сети, тем самым разграничивается информационная система. Снижается возможность уязвимости сразу всего сегмента физической сети.

Применение технологии виртуального сегментирования сети повышает уровень безопасности информационной системы, экономически выгодно по отношению к физическому сегментированию сетей, и при этом обеспечивает необходимый уровень взаимодействия частей системы. А также делает возможным расширенное управление информационными потоками в сети согласно определенным заранее правилам маршрутизации.

Биричевский А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СПОСОБ ПРИМЕНЕНИЯ ОТРИЦАЕМОГО ШИФРОВАНИЯ ДЛЯ ХРАНЕНИЯ КЛЮЧЕЙ

Нередко в средствах криптографической информации применяются резервные серии ключей. Резервные серии ключей вводятся в действие в случае компрометации основного комплекта ключей. Так как резервные серии ключей хранятся длительное время. Информация о наличии резервных серий ключевой информации может иметь значительную ценность для злоумышленника. Злоумышленником может быть организована атака на контейнеры ключевой информации. Предлагаемый способ хранения резервных серий ключей предполагает использование отрицаемого шифрование для сокрытия факта хранения дополнительных серий ключей.

В основе способа хранения ключевой информации лежит алгоритм отрицаемого шифрования, которой позволяет зашифровать два и более сообщений с двумя и более ключами в одном шифртексте.

Для хранения нескольких серий ключей предполагается использовать файл контейнера ключей. Данный контейнер представляет собой файл, который содержит в себе значение шифртекста. Для вычисления данного значения для серий ключей необходимо найти решение системы уравнений. В качестве алгоритма шифрования применяется ГОСТ 28147-89.

Для выбора конкретной серии ключей участники информационного обмена, которые хранят аналогичный контейнер ключей, договариваются о паролях, который используется для расшифрования основного и резервного ключа связи. В случае компрометации основного ключа связи, участники обмена переходят на резервный ключ связи, расшифровав резервный ключ связи резервным паролем. Так как длина файла шифртекста не зависит от количества зашифрованных серий ключевой информации, у злоумышленника отсутствует возможность доказать, что существуют несколько серий ключей.

Дополнительной положительной особенностью данного способа хранения ключевой информации является возможность совместить процесс генерации ключевой информации и

выработки файла контейнера ключей. В данном случае вычисление сводится к нахождению значений ключей шифрования ключей.

Стоит отметить, что данный метод может применяться только с учетом требований целевых алгоритмов шифрования для ключевой информации.

Рассмотренный способ хранения резервных серий ключей моет быть применен в средствах прикладного шифрования для сокрытия факта наличия резервных серий ключей.

Брагина Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

СОВРЕМЕННЫЕ СРЕДСТВА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Межсетевой экран (МЭ)– это комплекс аппаратных и программных средств компьютерной сети, осуществляющий контроль и фильтрацию пакетного трафика, поступающего из внешней сети, в соответствии с заданными правилами, определяющими условия прохождения пакетов с данными через границу из одной части общей сети в другую.

Межсетевой экран нового поколения (Next Generation Firewalls - NGFW) - это интегрированная программная платформа сети, которая сочетает в себе традиционный брандмауэр с другими функциями сетевых устройств фильтрации, такими как:

- распознавание и контроль приложений;
- предотвращение вторжений (IPS);
- наличие средства глубокой проверки пакетов (DPI);
- URL-фильтрация;
- распознавание контента и форматов данных;
- распознавание и использование учетных записей пользователей и групп;
- Дешифрование и инспекция SSL-трафика.

NGFW анализируют сетевой трафик в режиме реального времени – это обеспечивает надежную защиту против злоумышленников, вредоносного программного обеспечения, сетевых атак, попыток сетевого вторжения, краж данных, а также других видов сетевых угроз.

Наиболее распространенные межсетевые экраны следующего поколения: SecurityGeteway 21700 (разработчик – ChekPointSoftwareTechnologies), Cisco, McAfeeNextGeneration Firewalls, PaloAltoNetworks.

Присутствующий у продуктов всех представленных производителей функционал: NAT, PAT, прозрачный режим, режим анализа SPAN, возможность совмещения нескольких режимов работы на одном устройстве, StatefulInspection, защита от DoS/DDoS-атак, фильтрация трафика IPv6, фильтрация IP-пакет в соответствии с заданными правилами, настройка политики модификации трафика, поддержка VLAN по стандарту IEEE 802.1q, агрегация каналов, поддержка QoS, работа с сертификатами X.509, работа с каталогами пользователей, фильтрация одноранговых приложений, поддержка динамических групп адресов, фильтрация пакетов на прикладном уровне.

Рассмотрим межсетевой экран нового поколения, как защиту от угроз нулевого дня (0day).

Угроза нулевого дня – это не известные уязвимости, вредоносное программное обеспечение, защитные механизмы против которых на сегодняшний день не разработаны.

Большинство NGFW используют механизмы защиты, использующие сигнатурный анализ, однако некоторые содержат функционал вредоносного кода по поведению. Методы, применяемые межсетевыми экранами нового поколения, не охватывают весь спектр уязвимостей. Для проактивной защиты следует использовать такие технологии как песочница (специально выделенная среда для безопасного исполнения компьютерных программ), эмуляция кода (разбор программного кода на инструкции и имитацию их исполнения), эвристический анализ (обнаружение неизвестных вирусным базам вредоносных программ). Применение всего вышеперечисленного не даст возможности гарантировать то, что NGFW надёжно защищают от угроз нулевого дня. Но в определенном объеме задача защиты от угроз нулевого дня выполняется NGFW.

Брагина Е.К., Соколов С.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ОБЗОР ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ АНТИВИРУСНЫХ КОМПЛЕКСОВ

Антивирусный комплекс – это набор антивирусных программ, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. Антивирусное ядро – это реализация механизма сигнатурного сканирования и эвристического анализа на основе имеющихся сигнатур вирусов.

Существуют четыре вида антивирусных комплексов:

Комплекс для защиты рабочей станции. Устанавливается непосредственно на станцию и защищает ее от всевозможных вирусных атак. Включает в себя средства постоянной работы

(антивирусный сканер, постоянно проверяющий те файлы, которые необходимы операционной системе и сканер локальной почтовой системы, контролирующий входящую и исходящую почты) и средства, предназначенные для запуска с определенной периодичностью (антивирусный сканер, запускаемый по требованию пользователя либо программы).

Антивирусный комплекс для защиты файловых серверов. Устанавливается на сервере, который необходимо защитить от вирусов. Комплекс состоит из антивирусного сканера при доступе и сканера, который применяется только по требованию.

В антивирусном комплексе для защиты почтовых систем присутствуют антивирусы двух типов: непрерывно работающие средства (фильтр почтовых файлов, который будет проверять принимаемую и отправляемую информацию с сервера, на котором он установлен); фильтр почтового потока (отвечает за безопасность всего почтового потока сервера). В этот комплекс также входит сканер баз данных, именно он проверяет папки пользователей и их базы данных в реальном времени.

Комплекс, предназначенный для защиты шлюзов, проверяет поток данных, которые проходят через шлюз на наличие вирусов. Основные каналы, по которым вирусы могут «просочиться» в локальную сеть – это HTTP, SMTP, и FTP. Такой комплекс включает в себя в основном различные средства для постоянной работы. Средства, запускаемые по требованию, практически не используются, а если и используются, то только для защиты файлов сервера.

Наиболее распространенные антивирусные программные комплексы: антивирус Kaspersky; антивирус Dr.Web; антивирус Symantec Antivirus; антивирус McAfee; антивирус AntiVir Personal Edition.

	Dr.Web				Kaspersky		
	Защита файловых серверов	Защита почтовых систем	Защита шлюзов	Защита рабочих станций	Защита файловых серверов	Защита почтовых систем	Защита шлюзов
Платформа	Windows Linux Mac OS	Exchange Linux Domino	Linux	Windows Mac OS Linux	Windows Linux	Exchange Linux Domino	Windows Linux
Функции / возможности	Гибкое распределение нагрузки на файловую систему; выбор приоритета сканирования; выбор приоритета сканирования.	Антивирусная и антиспам-проверка почтовых сообщений, в том числе вложенных файлов, «на лету».	Эффективная фильтрация трафика на уровне ICAP-сервера; высокая масштабируемость.	Контроль за интернет-серфингом; защита в реальном времени; обнаружение всех видов угроз.	Поддержка виртуальных сред; совместимость и поддержка различного серверного ПО; защита в реальном времени.	Снижение нагрузки на корпоративную сеть; поддержка виртуализации.	Поддержка виртуальных сред; защита в режиме реального времени; поддержка Microsoft Forefront TMG.
Цена (10*1г.)	60’000	9’529,5	5’962,3	9’900	11’600	12’465	6’714

Все антивирусные комплексы используют сигнатурный анализ, следовательно, в обязательном порядке в них должно входить средство для поддержания антивирусных баз в актуальном состоянии. Во всех представленных выше продуктах от Dr. Web и Kasperskylab реализован механизм автоматического обновления.

В данной статье приведён минимальный обзор функциональности современных антивирусных комплексов. Однако выбирая защиту для организации, предприятия или учреждения, сочетая надёжность, стоимость и способность не влиять на основные функции, выполняемые сис темой лучше остановиться на антивирусных комплексах, использующих антивирусное ядро от Kasperskylab.

Булина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

О ПРОБЛЕМЕ ВНЕДРЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО КОДА НА WEB-САЙТАХ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ: НЕЙТРАЛИЗАЦИЯ ПРОБЛЕМЫ

Проблема несанкционированного доступа к информации на Web-сайтах посредством использования вредоносного программного кода злоумышленником, ведёт к нежелательным последствиям, возникающим как на стороне сервера, так и на стороне пользователей. Существование уязвимостей на большинстве современных платформах управления Web-контентом

даёт возможность злоумышленнику внедрить вредоносные файлы на сервер либо модифицировать уже существующие файлы.

Преступник в данной ситуации преследует следующие цели:

– использование Web-сервера для кражи имён пользователей и паролей;
– незаметная установка вредоносных программ на компьютер пользователя;
– переадресация на различный спам, ссылку на ресурс, содержащий вредоносное ПО и другие неправомерные действия.

Заражение Web-страниц начинается с того, что злоумышленнику необходимо получить непосредственно доступ к серверу. Здесь существует несколько методов получения доступа: словарная атака и эксплуатация уязвимостей.

Словарная атака – самый примитивный метод, требующий достаточное количество времени, основывающийся на подборе пароля «по словарю».

Эксплуатация уязвимостей – это использование уязвимостей кода, позволяющих загружать вредоносные файлы на сервер.

В силу вышеупомянутого текста следует выделить методы борьбы с вредоносным кодом на Web-сайтах, затрагивающие понятия: деактивации Web-сайта, резервная копия, эвристический метод поиска вредоносного кода.

Деактивация сайта - является важным моментом при начальной стадии борьбы с вредоносным кодом. Деактивация позволяет избежать дальнейшей работы злоумышленника.

Резервная копия – позволит восстановить содержимое сервера. Надо учесть тот факт, что резервная копия должна быть сделана до начала атаки.

Эвристический метод – основывается на некоторых предположениях, которые позволяют понять, что файл заражён.

Удаление обнаруженного вредоносного кода, которого в основном преступники шифруют, не исключает возможности появления похожих проблем в будущем, поэтому, что касаемо безопасности Web-сайтов, то необходимо сделать акцент на следующие действия:

– регулярная смена пароля, использование достаточно сложных паролей;
– создание резервных копий;
– проверка файлов;
– обеспечение безопасности ПК, управляющего Web-сайтом.

В последнее время наблюдается большой рост киберпреступности, которая является достаточно прибыльным делом для злоумышленников. Использование, так называемых, «уязвимостей нулевого дня», для которых ещё не созданы патчи, позволяет преступникам заражать целые компьютерные системы, использующие последние обновления без специальной защиты. Чтобы избежать внедрение вредоносного программного кода на сайт, помимо перечисленных действий, следует использовать для загрузки файлов на сервер протоколы SCP/SSH/SFTP вместо FTP, что позволит предотвратить пересылку паролей «в открытом виде». Если никак не бороться с заражением Web-сайта, то, в конце концов, поисковые системы могут выдать сообщение о том, что сайт является потенциально опасный и, тогда уже данный сайт будет помещён в специальную базу вредоносных сайтов.

Галанов А.И., Березин А.Н., Синёв В.Е.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наукСанкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПРОТОКОЛ УТВЕРЖДАЕМОЙ ГРУППОВОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ДВУХ ТРУДНЫХ ЗАДАЧ

Протоколы электронно-цифровых подписей (ЭЦП) широко применяются для придания юридической значимости электронным документам. Наиболее близкими к практике подготовки, визирования и утверждения бумажных документов в организации являются протоколы утверждаемой групповой электронной цифровой подписи (УГЭЦП). Данный тип протоколов позволяет сформировать ЭЦП руководителем от имени некоторого коллегиального органа. В протоколах УГЭЦП руководитель распределяет работу по подготовке электронного документа. После разработки каждый исполнитель формирует свою часть УГЭЦП, после чего отправляет её руководителю. Руководитель утверждает документ и формирует УГЭЦП.

В данном сообщении рассматриваются критерии для построения протоколов УГЭЦП и предлагается новый протокол, взлом которого потребует решения двух трудных задач.

В протоколах УГЭЦП обычно реализуется выполнение следующих требований: 1) готовить групповую подпись к документу может любое подмножество сотрудников коллегиального органа, от имени которого подписывается документ, причем результатом их действий является предподпись; 2) руководитель преобразует предподпись в конечную УГЭЦП, т.е. утверждает предподпись; 3)руководитель может определить перечень лиц, сформировавших предподпись, по значению УГЭЦП

и документу к которому приложена последняя; 4) внешние лица не могут установить, кто из сотрудников коллегиального органа формировал предподпись (а в частном случае и разрабатывал сам документ).

При разработке протокола УГЭЦП к перечисленным требованиям были добавлены следующие:

1) сотрудники при формировании своей части УГЭЦП используют только личные секретные ключи, которые неизвестны руководителю;

2) взлом протокола требует от атакующего решения двух независимых вычислительно трудных задач. Выполнение последнего пункта требований позволяет существенно повысить безопасность протокола.

В основе протокола лежит идея использования вычислительно трудной задачи дискретного логарифмирования по трудно разложимому модулю. Решение последней задачи требует одновременное решение задачи факторизации модуля и задачи дискретного логарифмирования по модулям, равным полученным простым делителям.

На первом этапе руководитель для каждого сотрудника, участвующего в процессе формирования УГЭЦП, генерирует рандомизирующие экспоненты, зависящие от открытого ключа последнего и подписываемого документа. Затем отправляет подписантам эти экспоненты, предварительно зашифровав их по открытым ключам подписантов. После этого руководитель формирует первый элемент УГЭЦП с использованием рандомизирующих экспонент и открытых ключей сотрудников, подписывающий документ.

Затем, каждый сотрудник, подписывающий документ, генерирует случайно число и направляет руководителю для формирования общего рандомизирующего параметра, на основе которого он формирует второй элемент УГЭЦП и рассылает каждому подписанту. Сотрудники, подписывающие документ, формируют свою часть коллективной преподписи на основе рандомизирующих экспонент, сгенерированного случайного числа и второго элемента подписи, и направляют свою часть преподписи руководителю.

На втором этапе руководитель осуществляет проверку корректности каждой части групповой преподписи и вычисляет свою часть групповой преподписи, а затем формирует на основе третий элемент УГЭЦП.

В качестве открытого ключа коллегиального органа выбирается открытый ключ руководителя, и проверка УГЭЦП осуществляется только по нему.

Для формирования рандомизирующих экспонент используются хэш-фунции. Это позволяет руководителю доказывать третьей стороне без раскрытия личного секретного ключа, что он правильно идентифицирует подмножество сотрудников, сформировавших преподпись к этому документу.

Горелочкина И.В., Белоусов А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ЭЛЕКТРОННЫЕ СИСТЕМЫ ДОКУМЕНТООБОРОТА КАК СРЕДСТВО ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Текущий анализ процесса делопроизводства показал, что в большинстве случаев делопроизводство выполняется на бумажной основе. Электронные системы документооборота не используются в большом объеме. Относительно делопроизводства существует ГОСТ Р 6.30-2003 «Унифицированные системы документации. Требования к оформлению документов». Создание документов, организация их движения и учета, а также последующее хранение должно строго соответствовать нормативным документам.

Обработка документов на бумажном носителе требует больших трудовых и физических затрат, также при обработке таких документов сотрудником возникает возможность ошибки в документе или вовсе утраты документа. Полный отказ от бумажного, безусловно, не возможен в ряде случаев, но перевод часть документов в электронную форму и постоянное отслеживание передвижения бумажных документов позволят исключить возможность утраты документа или передачи в ошибочное подразделение. Невозможность полноценного отслеживания документов дает возможность получения документов третьими лицами.

Для автоматизации делопроизводства необходимо внедрение электронной информационной системы, которая позволит создавать, хранить, учитывать вносимые туда документы, а также отслеживать бумажные документы. Электронная информационная система должна хранить в себе информацию обо всех документах, обрабатываемых в данной организации. Данная мера позволит автоматизировать процессы, связанные с делопроизводством, и повысит производительность труда.

Однако, доступ в такую систему третьих лиц или внесение заведомо неверной информации в электронную информационную систему, носит фатальных характер для информационной безопасности организации. Поэтому такие системы должны иметь четкое разграничение прав доступа и средства защиты от несанкционированного использования. Для обеспечения данных мер

необходимо составить матрицу доступа для каждого пользователя системы. В данной матрице должны быть четко регламентированные доступные действия, т.е. взаимодействие должно происходить по принципы «белого листа», при котором пользователю запрещены все действия, кроме «разрешенных».

Для предотвращения несанкционированного доступа необходимо обеспечить как минимум парольную защиту доступа. При этом использовать сложные пароли и регулярную смену паролей пользователей и администраторов. Желательно установить электронные средства защиты доступа.

Информация, хранимая в базе данных системы, должна быть зашифрована криптостойкими алгоритмами для предотвращения копирования или взлома. Необходимо обеспечить защиту оборудования, использования в информационной системе.

Ведение документооборота с помощью информационных систем позволяет улучшить процесс обработки, хранения и отслеживания документов, также повышается защищенность бумажных документов. Однако, сама электронная информационная система представляет большую угрозу информационной безопасности, получив доступ к которой возможна потеря всей хранимой информации, поэтому необходимо обеспечить должный уровень информационной безопасности системы.

Домбровская Л.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ХАРАКТЕРНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОВД

Оперативно-служебная информация ОВД, в частности данные уголовной регистрации, представляют существенный интерес для криминальной среды. Доступ к ней позволяет узнать, какой массив информации о преступной деятельности уже накоплен ОВД, а также появляется потенциальная возможность внесения несанкционированных изменений в совокупность идентификационных данных того или иного лица.

В связи с этим в деятельности ОВД существует угроза возникновения каналов утечки информации, причем существуют некоторые особенности, касающиеся источников формирования таких каналов.

Рассмотрим некоторые определения.

Утечка информации - это несанкционированный выход конфиденциальных сведений за пределы круга лиц, которым эти сведения доверены. По своей сущности утечка информации предполагает противоправное завладение злоумышленником конфиденциальной информацией и получение тем самым возможности ее использования в собственных интересах. Основными формами утечки информации являются ее разглашение, раскрытие и распространение.

Источник утечки защищаемой информации - это любой носитель конфиденциальной информации, к которому сумел получить несанкционированный доступ злоумышленник, располагающий необходимыми знаниями и техническими средствами для снятия информации, ее расшифровки и использования в своих целях в ущерб интересам ОВД.

Каналы утечки защищаемой информации – методы и пути утечки информации из информационной системы; нежелательная цепочка носителей информации, среди которых могут быть как злоумышленники и/или их специальная аппаратура. Анализ современной ситуации в сфере безопасности информации показывает, что в большей степени канал утечки информации – это скорее не техническое устройство, а социальное явление, или, учитывая, что социум весьма технически оснащен, – социально-техническое явление.

Классификация каналов утечки информации многообразна и зависит от принципа, положенного в основу классификационной группы.

В настоящее время принято рассматривать следующие основные виды каналов утечки информации:

1. Прямые и косвенные. Прямые каналы – это собственно злоумышленники, нарушающие правила хранения коммерческой и иной тайны, а также прямое копирование информации. Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы. Например, кража или утеря носителей информации, исследование не уничтоженного мусора; дистанционное фотографирование, прослушивание и т.п.

2. В зависимости от физических свойств и принципов функционирования каналы разделяются на:

– акустические – запись звука, подслушивание и прослушивание;

– акустоэлектрические – получение информации через звуковые волны с дальнейшей передачей ее через сети электропитания;

– виброакустические – сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– оптические – визуальные методы, фотографирование, видео съемка, наблюдение;

– электромагнитные – копирование полей путем снятия индуктивных наводок;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации «закладных устройств», модулированные информативным сигналом;

– материальные – информация на бумаге или других физических носителях информации

3. Технические каналы утечки информации.

4. Легальные каналы утечки информации и иные.

Большую роль в деле обеспечения информационной безопасности отводят техническим средствам. Однако их необходимо дополнять организационно-правовыми мерами, парольной защитой, криптографическими средствами. Только комплексная защита информации, создание и соблюдение требований политики безопасности в подразделениях ОВД обеспечат противодействие угрозам возникновения каналов утечки информации.

Ефимова А.Б.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войскМВД России

ЗАЩИТА ИНФОРМАЦИИ В ВЫСШИХ ВОЕННО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Внедрение компьютерной техники и информатизация образования привели к возникновению проблемы по организации защиты информации в высших военно-образовательных учреждениях.

В настоящее время в высших военно-образовательных учреждениях активно внедряются информационные системы, осуществляющие обработку персональных данных, делопроизводство, программы обучения и др. Эти системы предназначены для ведения базы данных курсантов, преподавателей и работников высшего военно-образовательного учреждения, оперативного управления учреждением.

Согласно Конституции Российской Федерации, Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовому кодексу РФ, при сборе персональных данных, операторами и третьими лицами, получающими доступ к персональным данным, должны обеспечивать конфиденциальность таких данных и постоянную защиту от несанкционированного хищения, изменения.

Защитить данную информацию в высшем военно-образовательном учреждении возможно при создании сильной организационной защиты информации – это регламентация деятельности взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Для построения информационной защиты в высших военно-образовательных учреждениях необходимо:

– разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных;

– сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, органами контроля и надзора и т.д.

Необходимо особое внимание уделить процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие:

– основания для такой передачи, предусмотренного федеральными законами, или согласия субъекта персональных данных, закрепленного, например, в договоре на оказание услуг;

– договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

Необходимо быть осторожным при размещении информации, содержащей персональные данные, на интернет-сайте высшего военно-образовательного учреждения.

С учетом выше изложенного можно определить следующие обязательные этапы работы по защите персональных данных:

1) определение всех ситуаций, когда требуется проводить обработку персональных данных;

2) выделение процессов, в которых обрабатываются персональные данные;

3) выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

4) определение круга информационных систем и совокупности обрабатываемых персональных данных;

5) проведение категорирования персональных данных и предварительной классификации информационных систем;

6) разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

7) внедрение системы обеспечения безопасности информации.

Следовательно, организационная защита информации в образовательном учреждении, сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;
– организацию системы защиты персональных данных;
– внедрение технических мер защиты персональных данных.

Таким образом, данная тема в настоящее время особенно актуальна, т.к. более активное использование средств компьютерной техники и в высших военно-образовательных учреждениях вызывает появление новых правовых проблем, требующих от учреждения принятия адекватных мер реагирования по устранению информационных угроз.

Жуковский Е.В., Москвин Д.А., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого»

ПРИМЕНЕНИЕ АНАЛИЗА ЭНЕРГОПОТРЕБЛЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ ПРОГРАММНО-АППАРАТНЫХ ЗАКЛАДОК В ОБОРУДОВАНИИ КОМПЬЮТЕРА

В настоящее время широкое распространение получили целевые компьютерные атаки (APT), целью которых является получение критической информации с компьютеров пользователей с использованием сложных трудозатратных векторов атак. В ходе развития информационных технологий, средства и подходы, применяемые для получения доступа к критической информации становятся все сложнее, и их реализация осуществляется на более низком уровне работы системы, где антивирусные и антируткитные средства не эффективны. С точки зрения сложности обнаружения, наибольшую опасность представляет вредоносное программное обеспечение (ВПО), внедренное во встроенное программное обеспечение оборудования (ПОО). Добавление скрытого недокументированного функционала в ПОО может осуществляться как в процессе его изготовления, так и на стадии эксплуатации оборудования. Так для модификации ПОО могут быть использованы уязвимости в архитектуре и прочих компонентах устройств, оставленные по халатности, или намеренно разработчиками и проектировщиками вычислительных систем и отдельных их компонентов.

Сложности в обнаружении данного типа ВПО обусловлены тем, что в случае компрометации оборудования, контролируемые защитным программным обеспечением компоненты операционной системы (ОС) могут оставаться неизменными, а выполняемые с оборудованием операции в рамках ОС не вызывать подозрения.

Актуальность данной проблемы подтверждается недавним обнаружением антивирусной компанией «Лаборатория Касперского» использования на практике описанного вектора атак, заключающегося в модификации встроенного ПО жесткого диска. Возможность проведения данной атаки была ранее описана в работах нескольких исследователей. Так же ранее в ряде публикаций была описана возможность размещения ВПО в других устройствах.

Предлагаемый подход к обнаружению закладок во встроенном программном обеспечении оборудования заключается в поиске аномалий в энергопотреблении устройства при взаимодействии с системой. Выбор для мониторинга именно такого параметра обусловлен тем, что выполняемые операции непосредственно влияют на картину энергопотребления, а использование других параметров функционирования системы, таких как, например, электромагнитное излучение, сопряжено с дополнительными сложностями измерения, и ограниченной областью практического применения. Возможность получения информации о характере выполняемых операций устройством по его энергопотреблению широко используется на практике в атаках на аппаратные криптографические устройства.

Предлагаемая методика обнаружения состоит из нескольких этапов. На предварительном этапе происходит сбор и анализ параметров энергопотребления устройства, целью которого является построение профиля энергопотребления. На последующем этапе происходит анализ энергопотребления и выявление отклонений в полученных значениях. Для анализа, полученного при измерении энергопотребления временного ряда можно применять различные подходы. Наиболее подходящими, исходя из постановки задачи, являются подходы из области глубокого обучения, такие как использование метода скользящего окна и разреженного кодирования. Полученные на предварительном этапе данные выступают в качестве обучающего набора для алгоритма. Используя разреженное кодирование, создается словарь всех фрагментов различной формы, которые встречаются в обучающем наборе данных и соотносятся с операциями, выполняемыми устройством. На этапе поиска аномалий, используя методы кластеризации, осуществляется подбор фрагментов из словаря, которые наилучшим образом соответствуют по форме каждому фрагменту исследуемого значения энергопотребления. Таким образом, из фрагментов словаря составляется новый, так называемый «восстановленный» сигнал, и путем сравнения его с исходными значениями, полученными в ходе мониторинга системы, осуществляется принятие решения о наличии или отсутствии закладки во встроенном программном обеспечении оборудования.

Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ ЭЛЕКТРОННЫХ КЛЮЧЕЙ

Донгл (от англ. **dongle**) — аппаратное средство, электронный ключ, предназначенный для защиты от нелицензионного использования и распространения программного обеспечения.

Электронный ключ представляет собой компактное устройство, подсоединяющееся к персональному компьютеру или мобильному устройству посредством портов ввода-вывода (порты USB, LPT, COM, BLUETOOTH, слоты PCMCIA, ISA, PCI). Программную часть составляет специальное ПО для работы с ключами. В его состав входят инструменты для программирования ключей, утилиты установки защиты и диагностики, драйверы ключей и др.

По устройству электронные ключи делятся на:

– Ключи, не содержащие встроенной памяти. Такие ключи не обеспечивают должную степень защищенности приложения.

– Ключи, содержащие только память. Этот класс ключей является морально устаревшим.

– Ключи на заказном ASIC-чипе. На сегодняшний день это самый распространенный класс ключей. Их функциональность определяется конкретным видом ASIC-чипа.

– Микропроцессорные ключи. В контроллер микропроцессорного ключа можно "прошивать" программу, реализующую функции, разные для каждого клиента. В принципе, любой микропроцессорный ключ легко можно запрограммировать так, что он будет работать по своему уникальному алгоритму.

Методы защиты, реализуемые в электронных ключах:

– Хранение в памяти ключа лицензий на программное обеспечение как вцелом, так и вразрезе отдельных его компонентов.

– Ограничение работы защищенных приложенийпо времени, количеству запускови т.п.

– Криптографические функции:

  – разработанные непосредственно производителями ключа (ASIC или собственные алгоритмы)

  – публичные алгоритмы AES (Rijndael), DES, GOST, ECC, PGP, и прочие.

– Функции контроля и предотвращения атак на защищенные приложения.

– Сетевые функции лицензирования.

– Функции защищенного обновления памяти ключа (как локально, так и удаленно).

– Средства выполнения кода защищаемого приложения внутри микроконтроллера ключа.

– Применение электронных ключей позволяет решить следующие задачи:

– Усовершенствовать процесс аутентификации (двухфакторная аутентификация) на локальном компьютере и в корпоративной сети, а также защищенный доступ к бизнес-приложениям.

– Зашифровать данные на серверах, ноутбуках и рабочих станциях.

– Обеспечить защиту персональных данных.

– Защитить электронную почту и взаимодействие с коллегами в системах электронного документооборота.

– Обезопасить финансовые операции в системах дистанционного банковского обслуживания (ДБО).

– Внедрить электронную цифровую подпись (ЭЦП) и защитить документы в системах сдачи электронной отчетности через Интернет.

– Обеспечить защиту корпоративного сайта в Интернет.

Пока разрабатывается и продается ПО, и стоит проблема компьютерного пиратства, защита программ останется актуальной. Что конкретно она будет представлять собой через некоторое время, сказать трудно. Но уже сейчас можно отметить некоторые тенденции, которые становятся очевидными.

Большую популярность приобретают USB-ключи, и они постепенно будут вытеснять ключи для параллельного порта. В ключах будут реализованы более сложные и стойкие алгоритмы, увеличится объем памяти.

«Двоюродные братья» электронных ключей - электронные идентификаторы, или токены, начинают широко применяться для аутентификации компьютерных пользователей. Такие устройства внешне похожи на электронные ключи для USB-порта, но отличаются большим объемом памяти, а также наличием алгоритмов шифрования. Токены в сочетании со специальными программами используются для авторизации пользователей при доступе к каким-либо информационным ресурсам (вход в локальную сеть, доступ к web-страницам и т. д.), для защиты электронной переписки (шифрование и электронно-цифровая подпись сообщений) и т. п.

Выбирая средство защиты, надо исходить из принципа экономической целесообразности. Защита должна выполнить свое основное предназначение - существенно сократить, а в идеале - прекратить, потери от пиратства, не сильно при этом увеличивая стоимость электронных ключей и программного продукта.

Иванов Д.В., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ИСПОЛЬЗОВАНИЕ КОНЦЕПЦИИ УПРАВЛЕНИЯ ПОТОКАМИ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ИНТЕЛЛЕКТУАЛЬНОГО ОКРУЖЕНИЯ

С каждым днем информационные технологии продолжают упрочнять свои позиции в самых различных сферах жизни современного человека. Понятие Интернета вещей позволило перейти от отношений человек-человек и человек компьютер к новому типу взаимодействия компьютер-компьютер.

Технология интеллектуального окружения (ambientintelligence, Aml) базируется на идеях Интернета вещей, и развивает их до концепции распределённой вычислительной сети устройств, предоставляющих естественный пользовательский интерфейс, скрывающий внутреннюю структуру. Такая система отвечает следующим требованиям:

- Учёт контекста взаимодействия;
- Персонализация;
- Адаптивность;
- Предугадывание поведения.

Таким образом, данная технология предоставляет новый способ применения разнообразных сетевых устройств для упрощения выполнения человеком повседневных задач, и использует для этого интеллектуальный механизм взаимодействия.

Данная технология может применяться для решения задач физической безопасности, поскольку система, способная учитывать контекст и предугадывать поведение позволит реализовывать более гибкое управление безопасностью, а так же уменьшить время реакции на нарушение.

С другой стороны, при реализации подобных систем, неизбежно произойдёт столкновение с новыми проблемами безопасности. Помимо тех, которые являются характерными для Интернета вещей, появляется риск утечки персональной информации. Распределённая сеть устройств, включающая в себя различные сенсоры, позволяет производить сбор информации об окружающей среде, в том числе и о находящихся рядом людях. Кроме того, поскольку технология подразумевает персонализацию, требуется хранение информации с привязкой к пользователю.

Отдельно стоит учитывать риски, связанные с работой интеллектуальных функций системы. Различные узлы подобных систем обладают разной степенью защищенности как от внешнего так и внутреннего нарушителя, в связи с чем компрометация слабозащищенного узла может стать угрозой для всей системы в целом.

Помочь справиться с этими проблемами может использование криптографии для хранения персональной информации о пользователе в закрытом виде, а также разработка модели управления потоками данных для обеспечения безопасности систем использующих технологию интеллектуального окружения.

Игнатов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ЭЛЕКТРОННАЯ ПОДПИСЬ КАК СРЕДСТВО ЗАЩИТЫ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

Электронная подпись – это современный, надежный юридический инструмент, позволяющий практически мгновенно, вне зависимости от времени суток и расстояний, заключить юридически полноценную сделку, а также в случае необходимости однозначно и без сомнений решить самые разнообразные споры. Электронная подпись является полноценной заменой рукописной подписи. Она обладает полной юридической силой согласно законодательству РФ. Для юридических лиц – это незаменимый инструмент, который позволяет наладить удобный и эффективный документооборот как внутри компании, так и с внешними предприятиями. Электронная подпись для физических лиц – это способ ускорить и упростить взаимодействие сгосударственными структурами, работодателями, учебными учреждениями через Интернет.

В Федеральном Законе от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» указано, что «Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию».

Смысл электронной подписи заключается в том, что для автора документа генерируется закрытый ключ – последовательность цифр определенной длины. Любой электронный документ с технической точки зрения также представляет собой последовательность цифр. ЭП представляет собой некое число, полученное в результате преобразования электронного документа как цифровой последовательности с помощью закрытого ключа автора. На базе закрытого ключа создается открытый ключ, доступный любому. Любой может проверить ЭП под документом при помощи соответствующих преобразований с использованием электронного образа документа, открытого ключа отправителя и собственно значения ЭП. Открытый и закрытый ключи однозначно связаны между собой, однако вычислить закрытый ключ по открытому практически невозможно, как минимум, это требует очень продолжительного периода времени.

Закрытый ключ, разумеется, содержится в тайне и известен только владельцу, чтобы никто, кроме владельца, не смог сформировать электронную подпись под документом. В то же время буквально любое заинтересованное лицо может проверить с помощью опубликованного открытого ключа, что документ подписал именно владелец, что документ не искажен, в противном случае меняется производная величина. Таким образом, подделать электронный документ, подписанный электронной подписью, существенно сложнее, чем документ на бумажном носителе. Защищенным оказывается и сам текст документа, причем не требуется помощи экспертов для выявления факта искажения документа. Проверка осуществляется строго математическим путем, причем автоматически, не нужно самому проделывать какие-либо вычисления. В результате запуска программы открытого ключа пользователь получает результаты проверки в наглядном виде как сообщение о том, что документ подписан таким-то лицом.

Рассмотрим плюсы электронной подписи:

– такую подпись крайне тяжело подделать, с ее помощью можно просто и очень быстро производить сделки;

– используя ЭП, пользователь имеет возможность быстро и без затруднений идентифицироваться;

– один человек или организация могут иметь несколько ЭП, С ее помощью легко контролировать целостность и достоверность документов;ЭП гарантирует высокий уровень защиты от подделок документации.

Из недостатков электронной подписи можно выделить следующее:

– такая подпись накладывает такие же обязанности, как и обычная подпись, ее нужно тщательно оберегать, так как есть вероятность «кражи»;

– невозможно отказаться от электронной подписи, если она уже подтверждена;

– чтобы ее получить нужно пройти несколько этапов оформления.

Существует три вида электронной подписи:

1. Простая электронная подпись (ПЭП) –предназначена для документооборота, позволяет подтвердить авторство, но не гарантирует неизменность документа после его подписания и не обеспечивают юридическую значимость.

2. Неквалифицированная электронная подпись (НЭП) – позволяет определить автора подписанного документа и доказать неизменность содержащейся в нем информации. В НЭП заложены криптографические алгоритмы, которые обеспечивают защиту документов.Такая подпись подойдет для внутреннего документооборота, а также для отправки электронных документов из одной компании в другую. Во втором случае, стороны должны заключить между собой соглашение, устанавливающие правила использования и признания электронных подписей.

3. Квалифицированная электронная подпись (КЭП) – обладает всеми признаками неквалифицированной, однако она может быть получена только в удостоверяющем центре, аккредитованном Минкомсвязи России. Программное обеспечение, необходимое для работы с КЭП, должно быть сертифицировано Федеральной службой безопасности. Следовательно, КЭП наделяет документы полной юридической силой и соответствует всем требованиям о защите конфиденциальной информацию.

Из всего вышесказанного можно сделать вывод, что в ближайшем будущем электронная подпись станет незаменимым техническим средством в электронном документообороте.

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

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСПЕТЧЕРИЗАЦИИ ПОЛЕТОВ САМОЛЕТОВ В ЗОНЕ АЭРОПОРТА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ «ВИРТУАЛЬНАЯ БАШНЯ»

Работа диспетчеров больших аэропортов характеризуется большой напряженностью, что приводит к опасным ошибкам в принятии решений. В докладе анализируется проблема создания наиболее комфортных условий для деятельности диспетчеров на основе использования трехмерного представления полетов в зоне аэропорта с высоты виртуальной башни (около тысячи метров).

Игнатьев М.Б., Кузьмин Д.В., Попов Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПАТТЕРНЫ ПОВЕДЕНИЯ ШЕСТИНОГО РОБОТА ПРИ ПЕРЕМЕЩЕНИИ ПО ПЕРЕСЕЧЕННОЙ МЕСТНОСТИ

В настоящее время широко развернулась роботизация вооруженных сил во многих странах мира, создаются мобильные роботы для участия в обороне и наступлении. В докладе рассматриваются паттерны поведения шестиногого робота при преодолении различных препятствий – рвов, заборов, узостей, лестниц и др.

Игнатьев М.Б., Жаринов О.О., Липинский Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ГАЗОПРОВОДОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АВТОНОМНОГО ШАГАЮЩЕГО АДАПТИВНОГО РОБОТА ДЛЯ ВНУТРИТРУБНОЙ ДИАГНОСТИКИ

Газопроводы протянулись на многие тысячи километров, они подвергаются деформациям и износу, что приводит к тяжелым авариям. В докладе анализируется проблема создания и использования автономного шагающего робота высокой проходимости для внутритрубной диагностики газопроводов.

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

БЕЗОПАСНОСТЬ ДОРОЖНОГО ДВИЖЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ АВТОМОБИЛЕЙ БЕЗ ВОДИТЕЛЕЙ

Развитие информационно-вычислительной техники позволило создать высокоавтоматизированный автомобиль – в пределе автомобиль без водителя. Человек-водитель является часто источником многочисленных дорожных аварий, каждый год на дорогах России погибает около 30 тыс. человек и 300 тыс. раненых. Появление автомобилей без водителей может кардинально изменить ситуацию на дорогах и повысить безопасность. В докладе анализируется структура и функции информационно-вычислительных систем высокоавтоматизированных автомобилей и определяется тактика и стратегия их использования.

Когтев А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

СОВРЕМЕННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В последнее время в мире появилась тенденция создавать комплексные системы защиты информации (СЗИ). Если раньше средства защиты информации (СрЗИ) и сетевые устройства как, например, межсетевые экраны и маршрутизаторы нужно было настраивать как отдельные фрагменты защищаемой автоматизированной системы (АС), то теперь под одной «обшивкой» CD/DVD диска может помещаться единый комплекс мер и СрЗИ, взаимодействующих и дополняющих друг друга, для охраны нужной системы. И эти средства зачастую уже являются не просто программными, а программно-аппаратными, защищая информацию, обрабатываемую в АС и средствах вычислительной техники (СВТ). Данными СрЗИ являются:

1) СрЗИ от несанкционированного доступа (НСД) (применяются для защиты от НСД к ресурсам АС со стороны лиц, имеющих непосредственный доступ к данной системе, то есть легальных пользователей АС);

2) средства криптозащиты (применяются для защиты информации по открытым каналам связи и когда есть возможность физического доступа посторонних лиц к защищаемым СВТ);

3) средства антивирусной защиты (применяются для защиты от компьютерных вирусов);

4) межсетевые экраны (применяются для защиты АС от НСД извне);

5) средства обнаружения вторжений (позволяют выявить подозрительную активность в АС);

6) система защиты от утечек (DLP-система, контролирует АС от фактов НСД и передачи информации за пределы защищаемой АС);

7) средства контроля защищённости информации, обрабатываемой в АС (применяется для проверки требований, предъявляемых к СрЗИ и защищаемой АС).

Защита информации (ЗИ) от НСД имеет 4 подсистемы:

1) управления доступом;

2) регистрации и учёта;

3) обеспечения целостности;

4) криптографическую.

В эти подсистемы входят такие важные составляющие как управление потоками информации, средства доверенной загрузки, учёт носителей информации, сигнализация попыток нарушения защиты, наличие средства восстановления СЗИ от НСД, очистка носителей информации и другие.

Из современных СЗИ, встречающихся на рынке, можно выделить несколько: SecretNet, DallasLock, Аура/Щит РЖД, Страж. Самые популярные системы это SecretNet и DallasLock. Первая система программно-аппаратная: в комплекте с диском идёт плата аппаратной поддержки (плата расширения) для запрета несанкционированной загрузки операционной системы с внешних съёмных носителей. И так как плата устанавливается в разъём системной шины, то SecretNet можно использовать только на стационарных компьютерах. В DallasLock плата расширения не

предусмотрена, поэтому продукт является программным, и при использовании в ноутбуках и прочих мобильных устройства конкуренции ему практически нет.

По сравнению с устаревшими СЗИ, современные отличаются высокой надёжностью. В них минимален процент сбоя. Но даже для внештатных ситуаций существуют средства восстановления СЗИ от НСД, проводятся периодические тестирования СЗИ от НСД и контролирующими органами (например, ФСТЭК) разрешено применение лишь сертифицированных СЗИ и СрЗИ. Но вместе с этим, современные СЗИ куда более сложные, и программно, и технически.

Можно предположить и в дальнейшем создание СЗИ, предлагающих покупателям комплексный подход к ЗИ АС, а также новые аппаратные СрЗИ, эффективно взаимодействующие с программной частью.

Лаврова Д.С., Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ КОРРЕЛЯЦИОННО-РЕГРЕССИОННОГО АНАЛИЗА

Развитие Интернета Вещей породило новые атаки на критически важные объекты и АСУ ТП, во многом представляющие собой техническую реализацию Интернета Вещей. В связи с огромным разнообразием существующих устройств, способных осуществлять коммуникацию и функционирование с использованием сети Интернет, появилось большое количество неизвестных атак, которые в настоящее время занимают лидирующую позицию среди прочих атак. Необходимость получения логических векторов для неизвестных атак тесно связана с задачей расследования инцидентов безопасности. Предлагается подход, аналогичный современным SIEM-системам, базирующийся на поиске взаимосвязей между событиями, сформированными из данных от устройств Интернета Вещей. Для обнаружения новых функциональных связей между устройствами Интернета Вещей, способных указать на взаимосвязь событий от данных устройств, используется метод корреляционно-регрессионного анализа. Корреляционный этап данного метода, основанный на анализе схожести изменений в динамике рядов данных от устройств, позволяет выявить нелинейные функциональные взаимосвязи. Регрессионный этап метода устанавливает аналитическую форму взаимосвязи, что в дальнейшем позволит выявить аномалии при регулярном мониторинге данной взаимосвязи, потенциально свидетельствующие об инциденте безопасности.

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ПРАКТИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

В настоящее время к проблеме обеспечения безопасности объектов топливно-энергетического комплекса (далее – ТЭК) приковано внимание различных специалистов, в том числе в области обеспечения информационной безопасности (ИБ). Для лиц, принимающих решения (ЛПР) важно принять во внимание всю совокупность требований, принятых на законодательном уровне: Федеральные законы, постановления Правительства, приказ ФСТЭК № 31.

Также важно принять во внимание, что введено понятие «Паспорт безопасности объекта ТЭК», в котором отражено требование: «оценки достаточности инженерно-технических мероприятий, мероприятий по физической защите и охране объекта при террористических угрозах…». Важно обеспечить унификацию при практической реализации требований указанных выше нормативных документов, а также требования «оценки», дополнительно применять современные стандарты ISO, реализующие замкнутый цикл PDCA и принятые в Российской Федерации в качестве ГОСТ Р – прежде всего стандарты серии 27001 и «целевой» стандарт для энергетики, который далее по каждому положению будет дополнять «базовый» ISO 27001 с целью дать полную методологическую основу создания СМИБ и/или ИСМ для СлПО ТЭК.

Для целей данной публикации отметим, что именно правильно определенные и категорированные активы «дают ключ» к корректному формированию перечня возможных актуальных угроз (в нотации ФСТЭК) и, соответственно, к реалистичной оценке возможного ущерба для СлПО ТЭК. В стандартах ISO изложена четкая логика данного процесса – выделенная совокупность ценных (критичных) активов, намеченных ЛПР к защите в составе СМИБ объектов ТЭК, требует определенных ресурсов для оценки уязвимостей, анализа соответствующих угроз, формирования файла рисков и плана обработки рисков.

В постановлении Правительства № 861 отмечено, что «субъект топливно-энергетического комплекса обязан представлять информацию об угрозе совершения и о совершении акта незаконного вмешательства на объекте топливно-энергетического комплекса…». Соответственно, подразумевается, что такой перечень угроз сформирован на основании Приложения 1 к указанному

выше постановлению Правительства, утвержден в установленном порядке и управляется на каждом СлПО ТЭК.

Представляется полезным сопоставить указанный выше перечень (Приложение 1) с перечнем типовых угроз согласно Приложения «С» стандарта, специально адаптированный для СлПО ТЭК и целям данной публикации. В Табл. 1 представлены 3 категории данных: перечень угроз согласно постановлению Правительства, выборка из перечня типовых угроз стандарта и оценка соответствующих последствий для указанных угроз. Для реализации процесса эффективной «отработки» последствий угроз для объектов ТЭК необходимо применять механизмы обратной связи (ОС), в том числе – с количественной точки зрения. Также важно, что все упомянутые стандарты ISO реализуют замкнутый цикл PDCA, который обеспечивает многовариантные ОС для обеспечения ЛПР в необходимой мере достаточным объемом количественных данных, например – метрик ИБ. Дополнительно важно отметить, что в постановлении уделено внимание важной технической задаче, реализация которой, как правило, отражена только в стандартах ISO – задаче управления записями в СлПО ТЭК. В частности, отражены требования для обеспечения защиты важных записей при предоставлении информации об угрозе, в зависимости от способа (средств): телефонной связи, радиосвязи, электронной или факсимильной связи. Также отметим, что в постановлении установлен конкретный месячный срок хранения носителей информации об угрозе, подтверждающих факт ее передачи, дату и время.

Таблица 1. Перечень угроз СлПО ТЭК

№ п.п.	Угроза (постановление Правительства 861)	Угроза (Приложение «С» стандарта 27005)	Последствия
1.	Угроза захвата	н/д	Вторжение в систему
2.	Угроза взрыва	н/д	Взрыв (терроризм)
3.	Угроза размещения или попытки размещения на объекте ТЭК взрывных устройств (взрывчатых веществ)	н/д	Взрыв (терроризм)
4.	Угроза поражения опасными веществами	Загрязнение	Вмешательство в систему
5.	Угроза блокирования	– Крупная авария – Пожар – Наводнение – Разрушение оборудования или носителей – Нарушение функционирования – программного обеспечения – Нарушение сопровождения информационной системы	Системный саботаж
6.	Угроза хищения	– Кража оборудования – Уничтожение оборудования или носителей	Хищение
7.	Угроза технического воздействия	– Авария системы – кондиционирования воздуха – или водоснабжения – Нарушение энергоснабжения – Отказ телекоммуникационного оборудования – Кража носителей или документов	Системная атака (отказ в обслуживании)

В тоже время в постановлениях Правительства не отражены в явном виде требования к обеспечению полного цикла управления рисками для организаций ТЭК. Также не предусмотрена оценка остаточного риска, которая позволяет дополнительно оценить уровень оценки защищенности активов СлПО ТЭК после применения выбранных мер (средств) обеспечения ИБ и определенного перечня рисков. Это обстоятельство может быть компенсировано как применением стандартов ISO, основанных на цикле PDCA, серии 27001, где требование менеджмента рисков установлено в явном виде, созданием ИСМ – с теми же требованиями или дополнительным внедрением «целевого стандарта» ISO серии 31000, который также принят в Российской Федерации как ГОСТ Р ИСО 31000-2010.

Для практической реализации требований защищенности СЛПО ТЭК необходимо принять во внимание важное обстоятельство – процесс проверки реализации определенного множества требований выполняется пошагово, и при выявлении ошибки (точнее, в терминах ISO –

несоответствия), выполняется локализация обратным процессом, начинаемым с той точки (исследуемого процесса, актива), где она выявлена. Для обеспечения безопасности объектов ТЭК, как уже было сказано выше, необходимо, чтобы процесс проверки (аудита) шел с адекватной скоростью, иначе общая «эффективная скорость» СМИБ (или ИСМ) снижается из-за более медленного процесса проверки (аудита). Второе важное обстоятельство (отражено в работе И. Пригожина), которое необходимо принять во внимание – при рассмотрении любого предмета (исследуемого процесса, актива), не следует стремиться к большей точности, чем допускает природа данного предмета.

Процесс обеспечения безопасности СлПО ТЭК рекомендуется реализовать на базе «классического» цикла PDCA, системы современных нормативных документов (ФСТЭК, постановлений Правительства и стандартов ISO). Предлагаемый подход позволит обеспечить необходимый уровень обеспечения безопасности СлПО, в том числе требуемый уровень информационной безопасности, адекватный современным требованиям к оценке угроз, анализу уязвимостей и полного менеджмента рисков на объектах ТЭК.

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СОВРЕМЕННЫЕ РИСК-ОРИЕНТИРОВАННЫЕ СТАНДАРТЫ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Практика выполненных проектов и общее состояние обеспечения безопасности на современном этапе показало, что при значительной стоимости активов организации, размер ущерба от реализации возможных инцидентов, как и размер стоимости комплекса средств (мер) обеспечения безопасности, могут создать определенный риск для устойчивости экономики организации, следовательно, необходимо контролировать определенный баланс этих переменных, который требует, в свою очередь, эффективных и достаточных управляющих воздействий.

Соответственно, необходимо выполнить анализ текущей экономической ситуации и предложить способ практической реализации, конкретно, эффективного управления издержками на основе менеджмента рисков и выявления скрытых ресурсов для определения источников экономического роста. Для обеспечения экономического развития организации целесообразно использовать риск-ориентированный подход, который сформулирован в ряде международных (ISO) и национальных стандартов (ГОСТ) [1 – 5]. Указанный подход основывается на формировании «контекста», который состоит, в общем случае, из внешних и внутренних факторов (аспектов), например, учитываются комплексные аспекты социально-экономических условий, в которых работает организация. В конечном итоге ожидается, что рациональный и систематический учет данных факторов приведет к повышению экономического роста организации. В частности, новая версия известного стандарта в области качества ISO 9001, которая ожидается в конце 2015 г. (http://www.iso.org/iso/home/standards/management-standards/iso_9000/iso9001_revision.htm), также содержит требования по анализу рисков, формирования четкой стратегии высшего руководства, направленной на удовлетворение потребностей заинтересованных сторон (“stakeholders”).

Например, в новом стандарте ISO 9001 версии 2015 г. отражены важные положения, напрямую способствующие понимаю предприятия своей ответственности по обеспечению экономического роста:

– Планируя систему менеджмента качества, организация должна принять во внимание проблемы и требования, и определить риски и потенциальные возможности, по которым должны быть предприняты действия, чтобы гарантировать, что система менеджмента качества может достигать ожидаемых результатов и предотвратить или уменьшить нежелательные последствия;

– Действия, предпринятые для обработки рисков и реализации возможностей, должны быть пропорциональны потенциальному влиянию на соответствие продукции и услуг;

– Организация должна управлять запланированными изменениями и анализировать последствия непреднамеренных изменений, принимая меры для снижения любого отрицательного эффекта, если необходимо;

– Организация должна установить и применять критерии для оценки, выбора, мониторинга деятельности и повторной оценки внешних поставщиков, основанные на их способности выполнять процессы или производить продукцию и услуги в соответствии с заданными требованиями;

– Продукция и услуги не должны поставляться потребителю, пока успешно не завершены запланированные мероприятия по проверке соответствия или пока поставка не санкционирована уполномоченным лицом и, там, где это применимо, потребителем.

Примем во внимание, что все современные стандарты ISO (действующие или находящие в статусе пересмотра) опираются на единый риск-ориентированный подход (на базе ISO 31000 [5]). Соответственно, важное преимущество современных систем менеджмента (например, систем менеджмента качества – СМК [1] или информационной безопасности – СМИБ [3]): требование

постоянного улучшения результативности, которое наилучшим образом способствует адекватной реакции системы на динамичные изменения ситуации, особенно проявления угроз. В частности, к критичным угрозам (изменениям) могут быть отнесены:

– Увеличение количества утечек чувствительной информации (коммерческой, технической, финансовой, персональной и пр.);

– Усиление критичных последствий утраты ценных для бизнеса активов;

– Усиление степени последствий блокирования работы критичных систем (финансовых, транзакционных, логистических, информационных и пр.);

– Невозможности быстрой замены, ремонта или покупки новой дорогостоящей импортной техники (технологий) или комплектующих.

В стандарте ISO 19011 [2] отмечается, в частности, что цели аудита могут быть сформированы на основании требований к оценке:

– уровня деятельности аудируемого объекта, отражающего степень повторяемости несоответствий или инцидентов;

– последствий имевших место внутренних и/или внешних происшествий, инцидентов;

– результативности систем менеджмента в отношении поставленных целей;

– степени выполнения правовых, законодательных, контрактных требований в системах менеджмента (“compliance”);

– аналогичных результатов, полученные на других объектах, позволяющие выявить тенденции (тренды).

Пример расчета эффективности ИСМ (в составе СМК и СМИБ), учитывающий стоимость активов организации, размер ущерба от реализации возможных инцидентов, стоимость комплекса средств (мер) обеспечения безопасности для снижения рисков и обеспечения экономического роста организации показан далее. Указанные выше переменные позволяют формировать управляемые условия для снижения рисков и, соответственно, минимизации издержек. В примере учитываются следующие ключевые переменные:

– стоимость защищаемых активов (“assets”);

– стоимость ущерба от реализации возможных инцидентов (“business impact”);

– уровень результативности системы менеджмента (“management system performance”);

– стоимость комплекса средств (мер) обеспечения безопасности (“controls”).

Макарова Е.Н., Горбунова Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОЦЕССЕ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

В настоящее время высокие компьютерные технологии позволяют за короткий срок узнать необходимую информацию, бурный ростом информатизации всех сторон жизни общества и государства является важной характеристикой современности.

Информация стала предметом преступных посягательств, получила свойство ценного товара, стали распространяться такие преступления как «хакерство» и компьютерные преступления. В свою очередь данный вид преступлений постоянно расширяется новыми направлениями и характеризуется высокой латентностью, отягчающейся сложностью установления и привлечения к ответственности виновных. В соответствии со сложившейся обстановкой информация тщательно охраняется, поскольку многие базы данных содержат информацию, которую в дальнейшем возможно использовать в преступных целях.

Для сохранения тайности информации создаются различные системы защиты информации, которые используются повсеместно, где существуют банки данных и большой поток информации. В настоящее время нет сто процентной гарантии о надежности созданных систем информационной защиты. Термин «информационная безопасность» можно определить как состояние защищенности в сфере использования информации. Одним из приоритетных направлений, где необходимо качественно повысить уровень данной безопасности, является правоохранительная сфера деятельности государства. Причиной такого обособления выступает то, что базы данных правоохранительных органов пользуются большим интересом среди правонарушителей и могут быть использованы ими в преступных целях. Помимо баз данных в правоохранительных органах находиться данные оперативных разработок, а так же сведения материалов уголовных дел и множество другой информации «утечка» которой может повлечь серьезные противоправные последствия.

Для сохранения сведений, нашедших отражение в материалах уголовных дел, на следователя налагается ответственность за сохранение служебной тайны. В предварительном расследовании существует такое понятие, как «тайна следствия», который включает в себя режим конфиденциальности информации. Помимо функции безопасности, тайна следствия имеет функцию защиты интересов и законных прав граждан, причастных к уголовному производству, ведь согласно Конституции РФ никто не является виновным в совершении преступления, пока суд не вынес ему

приговор. Ни следователь, ни другие лица не имеют права распространять сведения, связанные с расследованием уголовного дела. В полномочия следователя входит обеспечения информационной безопасности процесса предварительного расследования. Данную функцию следователь может выполнять в двух формах: процессуальной и не процессуальной. К процессуальной форме можно отнести предупреждение участников уголовного процесса за распространение информации, связанной с расследованием уголовного дела. То есть следователь доводит до лиц, которым известна какая-либо информация по расследуемому делу, их правовое положение, после чего выше указанные лица подтверждают данное действие подписью. Тем самым участники уголовного судопроизводства берут на себя ответственность за распространение конфиденциальных сведений, которая предусмотрена уголовным законодательством. К не процессуальной форме в свою очередь можно отнести тщательное фиксирование и хранение сведений, например хранение материалов уголовного дела в сейфе, предотвращение знакомства с ними посторонних лиц. Помимо всего, к непроцессуальной форме можно отнести этику документирования следственных мероприятий, которая обеспечивает бережное обращения с отраженной в них информацией. Не процессуальные действия, прежде всего самого следователя на половину обеспечивают сохранность сведений содержащихся в материалах уголовного дела.

Обеспечение режима информационной безопасности в процессе предварительного следствия, а так же всей правоохранительной деятельности выступает залогом своевременного и законного осуществления правосудия. Так как любые противоправные вмешательства в целях искажения или уничтожения информации относящейся к материалам уголовного дела, могут повлечь негативные последствия, необходимо более тщательно подходить к вопросу хранения конфиденциальных сведений всеми возможными способами. Помимо этого постоянно разрабатывать новые способы хранения информации и системы защиты информации.

Марков В.С., Сидоренко Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский научный Центр Российской академии наук

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Облачные технологии – технологии обработки данных, предоставляющие пользователю компьютерные ресурсы и мощности как интернет-сервис.

Для поддержки облачных вычислительных сред используются технологии виртуализации.

Использование технологии виртуализации позволяет существенно повысить эксплуатационные характеристики создаваемых информационных систем (ИС), задействовав при этом механизмы, заложенные непосредственно в аппаратной архитектуре процессоров, что фактически дает возможность любому пользовательскому приложению использовать вычислительные мощности, совершенно не задумываясь о технологических аспектах. Виртуализация серверов позволяет размещать несколько логических серверов в рамках одного физического, объединять несколько физических серверов в один логический для решения определенной задачи, например построения пула виртуальных приложений или создания кластера высокой производительности.

Вместе с тем использование технологий виртуализации сопряжено с рядом проблем, в том числе и в области обеспечения информационной безопасности (ИБ).

Угрозы, что свойственны физическим системам, актуальны и для виртуальных инфраструктур. При размещении информации в среде виртуализации к классическим угрозам безопасности прибавляется угроза несанкционированного доступа (НСД) к гипервизору. Реализованная атака на гипервизор позволяет получить доступ к данным всех виртуальных машин (ВМ), при этом выявить такую атаку трудно. Виртуальная машина по определению представляет собой программную систему, и ее легко можно подключить к такому же гипервизору на другой системе и получить полный доступ к локальным данным.

Одной из угроз виртуальной инфраструктуре, реализуемой через сеть передачи данных, является перехват данных при передаче по незащищённым каналам связи между облаком и клиентом.

Некоторые традиционные угрозы виртуальной инфраструктуре реализуются вследствие уязвимости физических серверов, на которых она развернута. В их числе сетевые атаки между виртуальными машинами в рамках одного хоста, подмена и/или перехват данных и оперативной памяти ВМ в процессе их миграции средствами виртуальной среды, вирусное заражение ВМ и использование их уязвимостей.

В работе рассматривается один из подходов обеспечения ИБ облачных технологий:

– для защиты от несанкционированного доступа рабочих мест пользователей, хостовой системы и системы хранения данных предлагается использовать традиционные сертифицированные средства защиты от НСД;

– для антивирусной защиты ВМ эффективнее использовать безагентный подход, обеспечивающий комплексную безопасность без установки агентского модуля в защищаемой

системе. В виртуальную среду внедряется виртуальное устройство – шлюз безопасности, который берет на себя функции антивируса для всех ВМ.

В этом случае антивирус работает на уровне гипервизора. Перенос антивирусной защиты на специально выделенное устройство существенно снижает расходование системных ресурсов, повышает производительность аппаратного обеспечения и увеличивает плотность ВМ на хост-сервере.

С появлением виртуальных сред появилась еще одна проблема – неконтролируемое сетевое взаимодействие между ВМ. Общая рекомендация такова: контролировать внешние подключения к среде виртуализации следует с помощью аппаратных решений, а внутренние – с помощью программных решений, реализуя, таким образом, комбинированный подход.

В отдельности каждые из этих защитных механизмов уже созданы, но они не собраны вместе для комплексной защиты облака, поэтому задачу по интеграции их в единую систему нужно решать во время создания облака.

Защита виртуальной инфраструктуры никогда не будет полноценной, если не обеспечить безопасность физической среды, включая непосредственные серверы виртуализации, а так же сеть передачи данных.

Если классические варианты защиты не подходят для самих облаков, то для защиты инфраструктуры, в котором облако находится, они вполне применимы.

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

ОТРИЦАЕМОЕ ШИФРОВАНИЕ НА ОСНОВЕ СТАНДАРТНОЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

В концепции отрицаемого шифрования рассматривается цель обеспечения достаточно высокой стойкости к принуждающим атакам. В модели таких атак предполагается, что атакующий имеет некоторый ресурс воздействия на отправителя, получателя или хранителя криптограммы, принуждающий последнего представить ключ расшифрования криптограммы. Стойкость к атакам с принуждением обеспечивается тем, что, по крайней мере, одно из зашифрованных сообщений не является секретным и атакующему предоставляется ключ, по которому расшифрование криптограммы приводит к раскрытию этого сообщения. При этом процедура расшифрования выполняется таким образом, что у атакующего нет обоснованных доводов, которые он мог бы привести в пользу утверждения, что с криптограммой связаны еще какие-то другие сообщения.

В настоящем сообщении рассматриваются новые критерии для построения алгоритмов ОШ, и предлагается новый способ отрицаемого шифрования на основе существующей инфраструктуры открытых ключей.

Основная идея ОШ основана на возможности расшифрования шифртекста с использованием различных ключей в различные сообщения, которые могут быть сформированы заранее.

В модели атак с принуждением, после того как отправитель выслал шифртекст получателю, атакующий может заставить и отправителя и получателя предоставить: 1) открытый текст, соответствующий отправленному шифртексту; 2) секретный ключ отправителя; 3) секретный ключ получателя; 4) алгоритм расшифрования, на выходе которого открытый текст зависит от каждого бита шифртекста.

Кроме этого существует так называемый активный атакующий, который может послать шифртекст, содержащий оба сообщения (фиктивное и секретное), и если получатель раскроет фиктивное сообщение, то получатель будет разоблачён.

Принимая во внимание вышесказанное, предложены следующие критерии для построения алгоритмов ОШ, стойких к активным двусторонним принуждающим атакам: 1) алгоритм должен состоять из двух интерактивных шагов и выполнять аутентификацию отправителя; 2) ОШ должно выполняться только с использованием открытого ключа получателя и случайных значений (т.е. процесс шифрования должен быть выполнен без использования открытого ключа отправителя или разделяемого секретного ключа); 3) для алгоритма отрицаемого шифрования должен существовать ассоциированный алгоритм вероятностного шифрования, который позволяет получить из открытого текста шифртекст неотличимый от шифртекста, порождаемого алгоритмом ОШ.

На основе предложенных критериев, был разработан новый алгоритм ОШ, использующий инфраструктуру открытых ключей. Пользователи генерируют свои открытые ключи на основе электронно цифровой подписи (ЭЦП) Эль-Гамаля, лежащей в основе отечественных и зарубежных стандартов ЭЦП. Предложенный алгоритм ОШ использует для шифрования открытый ключ получателя, а открытый ключ отправителя используется только для его аутентификации. Аутентификация отправителя позволяет определять активные атаки, в которых атакующий пытается инициировать протокол и представиться отправителем. Разработан ассоциированный алгоритм

вероятностного шифрования, который позволяет получать шифртекст, неотличимый от шифртекста, порождаемого разработанным алгоритмом ОШ.

Предложенный протокол ОШ отличается от существующих следующими свойствами: 1) стойкость к двухсторонней принуждающей атаке; 2) достаточно высокое быстродействие (в 2 раза медленнее алгоритма ЭЦП Эль-Гамаля); 3) содержит 2 этапа, на первом этапе производится аутентификация отправителя, на втором выполняется алгоритм ОШ; 4) получаемый шифртекст неотличим от шифртекста, порождаемого алгоритмом вероятностного шифрования; 5) размер шифртекста на 50% больше чем размер шифртекста, получаемого в случае использования алгоритма шифрования Эль-Гамаля с открытым ключом; 6) возможна реализация алгоритма с использованием вычислений на эллиптических кривых и существующей инфраструктуры открытых ключей.

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

ПРОТОКОЛ ШИФРОВАНИЯ НА ОСНОВЕ ДВУХ ТРУДНЫХ ЗАДАЧ ПО КЛЮЧУ МАЛОГО РАЗМЕРА

В применяемых системах защиты информации криптографические протоколы обеспечивают гарантированную стойкость шифрования информации при использовании ключей достаточно большого размера. На практике существует необходимость срочной передачи конфиденциальной информации, когда и отправитель и получатель имеют ключи малого размера (от 32 до 56 бит). Использование таких ключей в алгоритмах шифрования позволяет потенциальному нарушителю расшифровать шифртекст. В этом случае возникает задача обеспечения приемлемого уровня стойкости шифрования, при использовании ключей малого размера.

В данном сообщении предлагается новый протокол стойкого шифрования, обеспечивающий необходимый уровень стойкости при использовании ключей малого размера.

В основе протокола лежит идея использования протокола бесключевого шифрования, и разделяемого секретного ключа малого размера только для аутентификации отправленного шифртекста. Причём такой вариант применения ключа малого размера принципиально отличается от его применения в алгоритмах шифрования, так как у нарушителя будет лишь одна попытка угадать секретный ключ и навязать ложное сообщение.

Существующие протоколы бесключевого шифрования относятся к протоколам с открытым ключом, их безопасность основана на вычислительной сложности задачи дискретного логарифмирования (ЗДЛ), лежащей в их основе. Если рассматривать понятие безопасности как характеристику, учитывающую как стойкость криптографический механизмов, так и вероятность появления в обозримом будущем эффективных способов их взлома, основанных на прорывных достижениях в области решения вычислительно трудных задач. То существенное повышение безопасности может быть достигнуто путём разработки криптосхем, взлом которых потребует решения двух независимых трудных задач. Для этого ранее был предложен метод на основе использования составного модуля специальной структуры как в существующих криптосхемах, основанных на ЗДЛ, так и в разрабатываемых. Это позволило построить широкий спектр протоколов, для взлома которых потребуется решить две независимые вычислительно трудные задачи факторизации и задачи дискретного логарифмирования. Данный подход был применён для построения протокола шифрования по ключу малого размера.

В основе бесключевого шифрования лежат вычисления по простому модулю, которые являются коммутативными, в случае использования составного модуля вычисления по разным модулям не обладают свойством коммутативности, следовательно, значение составного модуля не может быть секретным и должно быть известно всем пользователям. Для этого было предложено использовать специальную схему формирования модуля, порождающего элемента и порядка, что позволило избежать некоторых видов атак, выявленных при разработке. Кроме этого процедуры коммутативного шифрования корректно работают только для сообщений, которые входят в циклическую подгруппу заданную порождающим элементом. При практическом применении требуется зашифрование самых различных сообщений, в том числе и случайных битовых строк, которые невозможно закодировать значениями из группы, как это можно сделать с фиксированным набором сообщений. Схожая проблема имеется и с разработкой алгоритмов коммутативного шифрования с использованием эллиптических кривых. Для решения этой проблемы был разработан механизм расщепления сообщений, позволяющий снять ограничения на шифруемые сообщения. Алгоритмы шифрования, использующие механизм расщепления сообщений можно отнести к классу вероятностных шифров, так как при шифровании используются случайные значения, а размер зашифрованного текста возрастает в два раза, но это позволяет существенно увеличить стойкость к некоторым атакам. Механизм расщепления сообщений позволил построить алгоритмы коммутативного шифрования, для взлома которых потребуется одновременное решение ЗДЛ и ЗФ, и с применением подхода,

использующего составной модуль специальной структуры, и встраивания алгоритма коммутативного шифрования Полига-Хеллмана. В качестве основных свойств предложенного алгоритма отметим: 1) для взлома потребуется решить ЗФ и ЗДЛ; 2) размер шифртекста увеличивается в 2 раза; 3) алгоритм относится к классу вероятностных шифров; 4) скорость работы сравнима с обычными алгоритмами бесключевого шифрования; 5) некоторые параметры должны быть известны всем участникам протокола.

Так как предложенный алгоритм относится к классу безключевых шифров, то необходимо обеспечить неразрывность процедур аутентификации и шифрования. Для этого было предложено использовать разделяемый секретный ключ малого размера. В качестве процедур аутентификации рассмотрено использование симметричных шифров, хэш-функций и имитовставок.

МорозовВ.Е., Дрозд А.В.
Россия, Москва, ООО «Новые Поисковые Технологии»

ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО КОМПЛЕКСА «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM» ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ ИЗ КОРПОРАТИВНЫХ СЕТЕЙ И КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В ОРГАНИЗАЦИИ

В настоящее время к современным средствам защиты информации, ориентированным на минимизацию внутренних угроз информационной безопасности, относят т.н. системы предотвращения утечки информации (DataLeakPrevention — DLP), внедряемые с целью выявления фактов нелегитимной передачи информации из защищенных автоматизированных систем.Основными преимуществами DLP-систем перед альтернативными решениями (продуктами для шифрования, разграничения доступа, контроля доступа к сменным носителям, архивирования электронной корреспонденции, статистическими анализаторами) являются:

– возможность контроля всех каналов передачи конфиденциальной информации в электронном виде, регулярно используемых в повседневной деятельности;

– обнаружение защищаемой информации по ее содержимому (независимо от формата хранения, каналов передачи, грифов и языка);

– возможность блокирования утечек (приостановка отправки электронных сообщений или записи на различные носители информации, если эти действия противоречат принятой в компании политике безопасности);

– автоматизация обработки потоков информации согласно установленным политикам безопасности (внедрение DLP-системы, как правило, не требует расширения штата службы безопасности).

Программный комплекс «Контур информационной безопасности SearchInform» (далее – КИБ) предназначен для выявления и предотвращения утечек конфиденциальной информации и персональных данных, а также для обнаружения фактов наличия конфиденциальной информации на компьютерах сотрудников и нерационального использования ими рабочего времени.

КИБ имеет клиент-серверную архитектуру. Под серверной частью подразумеваются платформы для перехвата данных (платформа SearchInformNetworkSnifferреализует сетевую подсистему иосуществляет перехват данных, пересылаемых пользователями по различным сетевым протоколам;платформа SearchInformEndpointSniffer реализует подсистему для защиты конечных точек сети иосуществляет перехват данных на уровне рабочих станций), под клиентской – приложения, предназначенные для поиска и просмотра перехваченных данных в целях проведения служебных расследований. Наличие единого поискового движка позволяет в полной мере использовать имеющиеся возможности по анализу перехваченных документов.

Взаимодействие основных компонентов КИБ осуществляется следующим образом:

– сервер NetworkSniffer анализирует сетевой трафик на уровне TCP/IP пакетов, осуществляет выделение в трафике контролируемой информации, производит идентификацию пользователей, сохраняет результаты перехвата в базы данных. Перехват данных поддерживается для следующих продуктов: MailSniffer (перехват почтового трафика), IMSniffer (перехват сообщений различных популярных IM-клиентов), HTTPSniffer (перехват файлов и сообщений, передаваемых по HTTP-протоколу), FTPSniffer (перехват документов, переданных и полученных по протоколу FTP), CloudSniffer (контроль входящих и исходящих данных, передаваемых на облачные сервисы), ADSniffer (анализа событий журналов безопасности ActiveDirectory);

– агенты EndpointSniffer устанавливаются непосредственно на рабочие станции пользователей. Перехват данных поддерживается для следующих продуктов:SkypeSniffer (перехват голосовых и текстовых сообщений, передаваемых при помощи Skype), DeviceSniffer (перехват информации, записываемой на USB-устройства и CD/DVD диски, а также их аудит и управление доступом к внешним устройствам), PrintSniffer (контроль содержимого документов, отправленных пользователем на печать), MonitorSniffer (снятие снимков и видеозапись экранов рабочих станций сотрудников), FileSniffer (контроль доступа к файловым серверам), HTTPSniffer, FTPSniffer, IMSniffer, MailSniffer, CloudSniffer, KeyloggerSniffer (перехват нажатий клавиш), MicrophoneSniffer (запись речи с

микрофона, входящего в состав компьютерной системы), ProgramSniffer (контроль активности сотрудников в процессе их работы с различными приложениями). Также агент EndpointSniffer может устанавливаться на мобильное устройство на базе iOS и осуществлять перехват данных, отправляемых/получаемых пользователем мобильного устройства (продукт MobileSniffer). Агенты передают данные не напрямую в базу или хранилище, а через серверы управления;

– перехваченная информация помещается в базы данных SQL или файловое хранилище. В частности, серверы NetworkSniffer (компоненты MailSniffer, IMSniffer, HTTPSniffer) и EndpointSniffer (компоненты SkypeSniffer, PrintSniffer, MailSniffer, MonitorSniffer, FileSniffer, MicrophoneSniffer, HTTPSniffer, IMSniffer, KeyloggerSniffer, LyncSniffer, ProgramSniffer, MobileSniffer) помещают перехваченные сообщения и файлы в базы данных, а компоненты FTPSniffer и DeviceSniffer используют для перехваченных данных хранилище;

– поскольку базы данных, хранилища и файлы на жестких дисках рабочих станций не обеспечивают быстрый доступ к данным, то для повышения производительности системы, перехваченные документы индексируются. Индекс – структура, обеспечивающая быстрый поиск по тексту и формальным признакам перехваченных документов;

– для управления индексами и базами данных компонентов КИБпредназначен продукт DataCenter. Известно, что по мере роста объема данных снижается скорость работы SQL-сервера и замедляется выполнение поисковых запросов, поэтому базы данных и индексы рекомендуется разбивать. DataCenter позволяет задать условия, по достижению которых будет автоматически создаваться новый индекс или база данных с настроенным на них перехватом. Также SearchInformDataCenter контролирует факт поступления перехватываемых данных в индексы и базы данных, работу компонентов КИБ, наличие свободного дискового пространства для работы системы и, в зависимости от настроек, извещает пользователя о различных событиях или неудовлетворительных условиях для функционирования системы;

– аналитические функции КИБ распределены между поисковым клиентом SearchInformClient, предназначенным для поиска по индексам и базам данных перехваченных документов; приложением SearchInformAlertCenter, предназначенным для автоматического мониторинга информационных потоков с возможностью уведомления сотрудника службы безопасности о случаях нарушения политик безопасности в отношении передаваемых данных и приложением SearchInformReportCenter, позволяющим формировать отчеты об активности пользователей и фактах нарушения политик безопасности (инцидентам).

Использование КИБ позволяет контролировать утечки документов, предотвращать применение «откатных» схем и подставных компаний, выявлять наличие нелояльных работников, людей, входящих в т.н. группы риска. Различные виды поиска, составление тематических словарей и работа с ними, использование регулярных выражений, библиотек цифровых отпечатков, формирование политик, ориентированных на контроль сотрудников и контроль документов, делают КИБ весьма удобным инструментом для решения проблем безопасности, возникающих в ситуации увольнения работников, для контроля документооборота, нерационального использования времени и ресурсов организации, проведения различных служебных расследований, планирования упреждающих и профилактических действий работников службы информационной безопасности.

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

КОНЦЕПЦИЯ БЕЗОПАСНОСТИСТЕК ТЕХНОЛОГИЙ ВЕБ-СЕРВИСОВ

Концепция сервисно-ориентированной архитектуры IT-технологии подразумевает реализацию бизнес-процессов предприятия в виде совокупности сервисов, взаимодействующих друг с другом, либо с пользователями в определенной последовательности и в соответствии с определенными правилами. Это нетривиальная задача - определить "определенную последовательность" и "определенные правила" таким стандартным для разработки приложений образом, чтобы охватить весь спектр существующих сценариев взаимодействия бизнес-объектов, учитывая исторически сложившееся многообразие технической и технологической реализации этого взаимодействия и самих бизнес-объектов. Решить эту задачу в рамках какой-либо единой технологии пока не удаётся. Хотя тенденция консолидации существующего множества технологий веб-сервисов в настоящее время налицо, для реализации сервисно-ориентированных архитектур с помощью веб-сервисов сейчас применяется совокупность технологий, образующих так называемый стек технологий веб-сервисов. Такой стек технологий веб-сервисов принципиально разбивается на следующие две составляющие:

– технологии, обеспечивающие функциональность веб-сервисов (Functions);
– технологии, обеспечивающие качество сервиса веб-сервисов (Qualityofservice).

Эти составляющие, в свою очередь, образуются несколькими слоями (layers):

Стандартные функциональные технологии:

– технологии, обеспечивающие функциональность веб-сервисов:

– транспортныйслой (transportlayer) - описывает средства обмена данными между веб-сервисами;

– коммуникационный слой (servicecommunicationlayer) - описывает средства формализации механизмов использования транспортных протоколов веб-сервисами;

– слой описаний сервисов (servicedescriptionlayer) - описывает средства формализации интерфейсов веб-сервисов с целью обеспечения их функционирования независимо от программно-аппаратной платформы реализации или языка программирования;

– сервисныйслой (servicelayer) - описывает программное обеспечение, вызываемое с помощью WSDL-описаний интерфейсов веб-сервисов;

– слой бизнес-процессов (businessprocesslayer) - описывает возможности организации веб-сервисов для реализации бизнес-процессов и потоков работ;

– слой реестров сервисов (serviceregistrylayer) - описывает возможности организации веб-сервисов в иерархические библиотеки, позволяющие публикацию, поиск и вызов веб-сервисов поих WSDL-описаниям интерфейсов.

Технологии, обеспечивающие качество сервиса веб-сервисов:

– слойполитик (policylayer) - Описывает правила и условия, согласно которым веб-сервисы могут быть использованы;

– слойбезопасности (security layer);

– слойтранзакций (transaction layer);

– слойуправления (management layer).

Представленный выше стек технологий веб-сервисов вводит иерархию во множество технологий веб-сервисов в соответствии с их функциональным назначением, в перечне указаны лишь наиболее широко применяемые и устоявшиеся технологии. Стандартными названы технологии, получившие официальный статус в стандартах международных консорциумов по разработке IT-стандартов (W3C). В действительности, спектр технологий, описывающих аспекты использования веб-сервисов и сервисно-ориентированных архитектур, крайне широк. В частности, поскольку процесс разработки данных технологий является открытым, любая компания, некоммерческое объединение специалистов или даже один специалист могут разработать и опубликовать спецификацию разработанной им технологии, что стало серьезной проблемой для рынка веб-сервисов - количество спецификаций стало столь велико, что при фактической нерегламентированности повсеместного процесса их разработки, ввода в действие и использования, появляется опасность ввергнуть индустрию в технологическую разобщенность и хаос. Тогда как технологическая разобщенность - как раз то, от чего, прежде всего, хотели уйти разработчики веб-сервисов.

Представляется целесообразным при проектировании и реализации бизнес-процессов предприятия формировать концепцию безопасности политик, правил и последовательности для совокупности стандартных функциональных и сервисных технологий, которые установят согласованный стек технологий веб-сервисов как сервисно-ориентированную архитектуру IT-технологии, применяемой для решения задач предприятия.Эти же правила распространяются на Слой безопасности, который отвечает за безопасность веб-сервисов (авторизации, аутентификации и разделение доступа).

В представленном примере на основе разработанного математического аппарата [6 – 7] учитываются численные метрики (важно, что именно количественные оценки), которые позволяют варьировать показатели защищаемых активов организации: (определены активы начальной стоимостью 1.000.000 руб.), стоимость комплекса средств (мер) обеспечения безопасности (определена начальная стоимость 180.000 руб.), и 4 значения результативности реализованных средств (мер) обеспечения безопасности (определяемых, например, по результатам всех типов аудитов ИСМ (внутренних и внешних) – 0,5; 0,7; 0,9 и 0,99).

Предположим, что количество инцидентов безопасности, способных нанести ущерб активам организации, растет неравномерно в течение года (по закону, близкому к экспоненциальному) и, в определенный момент, если не предпринять адекватных действий, может сравняться со стоимостью активов организации, т.е. полностью разрушить бизнес [4]. Необходимо отметить, что стандарт [4]содержит требования к обеспечению непрерывности бизнеса и предлагает ряд сценариев для управления возможными воздействиями (“business impact”).

Рассмотрим пример противодействия негативным факторам (инцидентам безопасности) для ИСМ: на 8 месяце размер потенциального ущерба от инцидентов безопасности Синц составит 420.000 руб. (правая шкала), что уже превышает стоимость реализованного комплекс средств (мер) обеспечения безопасности Смоб (180.000 руб.), стоимость активов организации Сакт составляет 1.000.000 руб., степень результативности системы безопасности ИСМ РИСМ определим равной 0,7.

В данном примере актуальная стоимость активов организации АИСМ (благодаря реализованному комплексу средств (мер) обеспечения безопасности), составит:

АИСМ = С акт – С моб – Синц * (1 – РИСМ) = 1.000.000 – 180.000 – 420.000*0,3 = 694.000 руб.

Заметим, что без внедрения комплекса средств (мер) обеспечения безопасности стоимость активов АИСМ при Смоб = 0 и том же размере Синц составит:

АИСМ = С акт – С инц = 1.000.000 – 420.000 = 580.000 руб.

Отметим, что с увеличением времени работы ИСМ (в составе СМИБ и СМК) экономическая эффективность будет только возрастать, кроме того, будет накапливаться положительный опыт противодействия попыткам негативного воздействия на ценные активы организации, что в конечном итоге повышает оценку результативности системы безопасности СМИБ и, как следствие, общую устойчивость бизнеса.

Применение современных риск-ориентированных систем менеджмента позволяет формировать экономические оценки, основанные на постоянном измерении результативности, что обеспечивает условия для снижения издержек и повышения экономической устойчивости организации даже в условиях экономической нестабильности.

Радченко Н.В., Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ОПЫТ ИССЛЕДОВАНИЯ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ПРИ ТЕСТИРОВАНИИ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОДА

В работе проведен анализ существующих типовых подходов к построению инструментальных сред анализа безопасности программного кода, в результате которого выделены следующие основные способы решения поставленной задачи:

– в качестве исходной информации о структуре исследуемой программы используется отладочная информация компилятора;

– т.к. компилятор для получения отладочных данных выполняет лексический, синтактический и семантический анализ, то он применяетсядля разбора. Такое решение заставляет обращаться к компиляторам с исходным текстом, включая, gcc (GNUCompilerCollection). Его достоинством следует считать оптимизированный коди, следовательно, скорость выполнения разбора сравнима со скоростью компиляции и сборки;

– время сбора информации о структуре программы может бытьуменьшено за счет отсутствия необходимости генерации кода, но увеличивается на время записи полученных данных в базу данных. В исходный компилятор вставляется функция, которая генерирует sql-запросы для лексем, затем записывает их в отдельный файл. После завершения работы измененного компилятора запускается программа, выполняющая все созданные запросы;

– запросы записываются в реляционную, преимущественно проприетарную СУБД, например, PostgreSQL;

– структуру самой БД каждый разработчик-исследователь определяет исходя из своих задач, но минимальнов базах присутствует информация о переменных, процедурах, функциях, линейных участках, методах, классах и связях между ними. Дополнительно в комплексах присутствуют таблицы для опасных функций, свойственными конкретному языку и, подлежащие записи вручную;

– после сбора сведений о структуре программы выполняется её запуск с целью контроля выполнения функций. Технология вставки датчиков существенно уступает запуску под отладчиком, поэтому при разработке комплексов анализа кода наблюдается тенденция к использованию в испытательных лабораториях инструментов на базе такого мощного отладчика, как GNUDebugger. Чтобы можно было его использовать, указанный ранее компилятор, собирает исполняемые файлы с отладочной информацией (например, COFF) и затем они запускаются в виртуальной среде с работающим отладчиком;

– отладчик формирует журнал срабатывания функциональных возможностей, что необходимо для сравнения с имеющейся последовательностью в БД, определенной на стадии статического анализа. Дополнительные программы разрабатываются для выполнения сравнения;

– при помощи собственных программ построения алгоритма работы, на базе сведений о взаимосвязи между функциональными объектами формируется визуальное представление, чаще всего носящее номинальный характер и не пригодный для ручного разбора работы выполнения программы. Несмотря на это, нынешний уровень решения данной задачи позволяет выделять на данной графической схеме те участки кода, которые содержат опасные функции из таблицы БД;

– задача анализа программ, не имеющих исходного текста, решается при помощи эмулирующих отладчиков, в частности, обоснованная популярность у «Bochs», являющегося некоммерческим продуктом с исходным кодом, со встроенным отладчиком, поддерживающим неограниченное количество виртуальных точек останова и функций обратной трассировки.

В основной статье рассматривается функциональная структура комплексов, создающихся по принципу сбора готовых решений с открытым исходным кодом и интеграции в единую среду отладки и анализа программ. Анализируются положительные и отрицательные стороны, как подхода, так и конкретных решений, включая ограниченность применения версией модифицированного компилятора, зависимость от структуры отладочной информации, не позволяющей сделать более высокую детализацию, высокая эффективность бездатчикового подхода при анализе драйверов и прошивок, а также сложности распространения однажды созданной тестовой среды на анализ новых программ.

Редковников В.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД

В ОВД собирается, обрабатывается, хранится и используется большое количество персональных данных сотрудников ОВД, начиная от такой информации, как дата и место рождения сотрудников, и заканчивая информаций об их имуществе. В связи с этим возникает проблема обеспечения сохранности этих персональных данных. В настоящее время данной проблеме уделяется достаточно большое внимание.

Согласно статье 39 федерального закона РФ от 30.11.2011 № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» ОВД вправе получать, хранить, обрабатывать, использовать и передавать персональные данные сотрудников ОВД, вести их личные дела, документы учёта, а также банки данных. Согласно этой же статье данные сотрудников ОВД являются служебной (государственной) тайной, а следовательно ОВД обязан обеспечить защиту этих персональных данных от неправомерного их использования или утраты.

Согласно статье 11 и статье 17 федерального закона РФ от 07.02.2011 № 3-ФЗ «О полиции» ОВД вправе использовать для работы с персональными данными сотрудников ОВД специальные информационные системы. Чаще всего данные информационные системы реализуются в виде категорированных компьютеров.

К данным категорированным компьютерам применяются специфические требования. Согласно Руководящему документу Гостехкомиссии России от 30.03.1992 «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» категорированные компьютеры должны обеспечивать:

– идентификацию, проверку подлинности и контроль доступа субъектов в систему, к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, к программам, томам, каталогам, файлам, записям, полям записей;

– управление потоками информации;

– регистрацию и учёт входа (выхода) субъектов доступа в (из) систему(ы) (узел сети), выдачи печатных (графических) выходных документов, запуска (завершения) программ и процессов (заданий, задач), доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи, доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей, изменения полномочий субъектов доступа, создаваемых защищаемых объектов доступа;

– учёт носителей информации;

– очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;

– сигнализацию попыток нарушения защиты;

– шифрование конфиденциальной информации;

– шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах;

– использование аттестованных (сертифицированных) криптографических средств;

– целостность программных средств и обрабатываемой информации;

– физическую охрану средств вычислительной техники и носителей информации;

– наличие администратора (службы) защиты информации в автоматизированных системах;

– наличие средств восстановления систем защиты информации от несанкционированного доступа.

Только в случае выполнения всех вышеперечисленных требований будет обеспечен должный уровень безопасности персональных данных сотрудников ОВД.

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

ШИФРОВАНИЕ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ПО РАЗДЕЛЯЕМОМУ КЛЮЧУ МАЛОГО РАЗМЕРА

В случае необходимости передачи конфиденциальных сообщений по открытым каналам при наличии у отправителя и получателя общего секретного ключа малого размера (например 32, 40 или 56 бит) непосредственное шифрование сообщений по разделяемому ключу не является безопасным, поскольку, перехватив криптограмму, нарушитель имеет практическую возможность нахождения ключа путем перебора по ключевому пространству. Однако ключ такого размера находит интересное применение в протоколах, включающих использование симметричной и ассиметричной криптографии.

Так, в протоколах обмена зашифрованными ключами (encryptedkeyexchange, EKE) секретный ключ малого размера (например, пароль) используется для шифрования генерированного случайным образом открытого ключа. При реализации этого протокола со схемой открытого распределения ключей Диффи-Хелмана (DH-EKE) тем самым решается проблема атаки «человека по середине» и далее обеспечивается аутентификация сторон путем шифрования передаваемых данных общим секретным ключом.

Недавно был предложен протокол стойкого шифрования по ключу малого размера на основе комбинирования протокола бесключевого шифрования и аутентификации передаваемых в рамках протокола бесключевого шифрования данных путем их шифрования общим секретным ключом малого размера. С целью повышения производительности процедур коммутативного шифрования интересна реализация этого протокола в конечных группах точек эллиптической кривой, заданной над конечным полем.

Но в отличие от схемы открытого распределения ключей Диффи-Хелмана и ряда других алгоритмов ассиметричного шифрования, которые естественным образом можно "переложить" на эллиптические кривые - реализация алгоритма коммутативного шифрования (АКШ) на ЭК сталкивается со следующей проблемой. При шифровании обычно предполагается, что любое сообщение, размер которого не превосходит некоторое заданное значение, может быть корректно зашифровано и расшифровано, т.е. на входные значения АКШ не накладывается ограничений. Данное требование трудно реализовать при разработке АКШ с использование ЭК, заданных над конечными полями. Причиной этому является то, что координаты точек ЭК должны удовлетворять некоторому уравнению третьей степени, а значит, не все пары значений соответствуют точкам ЭК.

Для решения этой задачи предлагается способ вероятностного кодирования точек ЭК, в котором шифруемое сообщение интерпретируется как часть абсциссы точки ЭК, к которой присоединяется оговоренное число случайных бит. Полученное значение принимается за абсциссу и проверяется существование точки ЭК с данным значением абсциссы. Если такой точки на используемой ЭК не существует, то генерируется новая случайная последовательность бит и проверка повторяется. Если такая точка существует, то вычисляется ее ордината. Задаваемые таким образом точки шифруются с помощью АКШ. Сообщение извлекается из расшифрованной точки путем удаления из значения ее абсциссы добавленного при шифровании числа бит. Криптограмма имеет размер незначительно больший, чем размер исходного сообщения (на 7%). Предложенный способ вероятностного кодирования позволяет реализовать коммутативную функцию шифрования в протоколе бесключевого шифрования на ЭК, и, далее, протокола стойкого шифрования по ключу малого размера на ЭК (механизм аутентификации передаваемых в процессе бесключевого шифрования сообщений реализуется без изменений).

Но анализ полученного протокола выявил серьезный недостаток, позволяющий пассивному злоумышленнику при наличии достаточного числа перехваченных сообщений восстановить секретный ключ малого размера.

Необходимым условием для возможности многоразового использования секретного ключа малого размера в предложенном протоколе бесключевого шифрования, как и в протоколах обмена зашифрованными ключами, является псевдослучайность (вычислительная неотличимымость от случайных значений) передаваемых шифртекстов, что предотвращает получение атакующим данных, использование которых позволяет осуществить многократную проверку предполагаемых значений разделяемого секретного ключа.

Действительно, шифрование данных такого типа приводит к получению криптограмм, по которым определить короткий ключ шифрования методом перебора по пространству возможных ключей не представляется возможным, поскольку каждый из испытуемых ключей приведет к восстановлению из криптограммы некоторого случайного (псевдослучайного) исходного текста. Для атакующего каждое допустимое значение ключа является равноправным, т.е. у него нет вычислительно эффективного критерия отбраковки неверных значений ключа.

В случае же реализации протокола на ЭК у атакующего есть такой критерий - передаваемое сообщение, до шифрования секретным ключом малого размера, соответствовало абсциссе точки ЭК. При разработке способа вероятностного кодирования было показано, что случайное значение является абсциссой точки ЭК с вероятностью ½, что позволяет злоумышленнику - методом перебора по пространству возможных ключей и проверкой полученного значения на соответствие точке ЭК - уменьшать множество возможных значений ключа в два раза на каждом перехваченном сообщении.

Таким образом, для нахождения значения ключа необходимо число перехваченных сообщений, равное битовой длине ключа.

С учетом указанного недостатка предложенный протокол исключает повторное использование общего ключа малого размера, но при разовом его использовании позволяет гарантированно защищенно передать сообщение.

Смирнова О.Г., Хитов С.Б.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России,
Санкт-Петербургский университет ГПС МЧС России

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СПОСОБ РАЗРАБОТКИ ЭФФЕКТИВНЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Угроза защищаемой информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. То есть угроза информации обусловлена вполне определенными факторами, совокупностью явлений и условий, которые могут сложиться в конкретной ситуации. Выявление и анализ угроз защищаемой информации является ответственным этапом при построении системы защиты информации и разработке политики безопасности на предприятии.

Любая угроза состоит из определенных взаимосвязанных компонентов, каждый из которых сам по себе не создает угрозу, но является неотъемлемой ее частью.

Угрозы защищаемой информации связаны с ее уязвимостью, или неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим ее статус.

Реализация угроз приводит, в зависимости от их характера, к одной или нескольким формам проявления уязвимости информации. Набор взаимосвязанных между собой компонентов угрозы предопределяет конкретную форму.

Определяющим признаком угрозы является ее направленность, или результат (негативное последствие), к которому может привести дестабилизирующее воздействие на информацию.

Этим результатом во всех случаях реализации угрозы является нарушение статуса информации.

По видам угрозы чаще всего подразделяют на два основных класса:

– естественные;
– искусственные.

Самым непредсказуемым видом дестабилизирующего воздействия являются естественные угрозы, так как они не зависят от воли человека и связаны с природными, биологическими и техническими угрозами.

В качественном изменении климата на всей территории европейского континента данный вид угроз становится все более критическим.

К сущностным проявлениям угрозы, относятся:

– источники дестабилизирующего воздействия на информацию (от кого или от чего исходит дестабилизирующее воздействие);

– виды дестабилизирующего воздействия на информацию (каким образом (по каким направлениям) происходит дестабилизирующее воздействие);

– способы дестабилизирующего воздействия на информацию (какими приемами, действиями осуществляются (реализуются) виды дестабилизирующего воздействия).

Источники дестабилизирующего воздействия подразделяются на:

– антропогенные;
– техногенные;
– стихийные.

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди, которые делятся на следующие категории:

– сотрудники данного предприятия;

– лица, не работающие на предприятии, но имеющие доступ к защищаемой информации предприятия в силу служебного положения (из вышестоящих, смежных (в том числе посреднических) предприятий, контролирующих органов государственной и муниципальной власти и др.);

– сотрудники государственных органов разведки других стран и разведывательных служб конкурирующих отечественных и зарубежных предприятий;

– лица из криминальных структур, хакеры.

Поскольку виды и способы дестабилизирующего воздействия зависят от источников воздействия, то и причины, обстоятельства (предпосылки) и условия должны быть привязаны к источникам воздействия.

Применительно к людям причины, обстоятельства и условия,как правило, увязаны с характером воздействия — преднамеренным или непреднамеренным.

Анализ возможных угроз и разработка мер и методов защиты информационного статуса организации поможет создать эффективную комплексную систему защиты информации, а так же поможет создать баланс жизненно важных интересов сотрудников и организации.

Солодянников А.В., Пилипов М.В., Парамонов А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРИМЕТРА АВТОМАТИЗИРОВАННЫХ КАРТОГРАФИЧЕСКИХ СИСТЕМ

Особенностями автоматизированных картографических систем (АКС), влияющими, в общем случае, на мероприятия по защите информации являются:

– наличие сегментов АКС с различным уровнем конфиденциальности обрабатываемой информации;

– двухстороннее взаимодействие (получение геопростанственной информации из нескольких источников, передача пространственных данных потребителям)с сетями общего пользования;

– применение в качестве банка исходных данных единой системы геопространственной информации (открытой и закрытой);

– конечными потребителями картографической продукции могут быть как отечественные (органы государственной и исполнительной власти, юридические и физические лица), так и зарубежные потребители;

– необходимость ведения учета картографической информации.

Исходя из вышеизложенного, одной из функций, выполняемой системой защиты информации АКС, является защита периметра автоматизированной картографической системы.

Под периметром АКС следует понимать:

– границу контролируемой зоны (периметр охраняемой территории организации), внутри которой размещаются технические средства, входящие в состав АКС;

– физические каналы (включая беспроводные), по которым может циркулировать информация, обрабатываемая в АКС, имеющие выход за пределы контролируемой зоны.

Отдельным элементом, который необходимо учитывать при формировании требований к системе защиты периметра, является использование внешних (съемных) накопителей информации.

Защита периметра АКС должна обеспечивать невозможность (существенное затруднение):

– несанкционированного доступа к ресурсам защищаемой системы как от злоумышленников, так и от легальных пользователей;

– сетевых атак, направленных на недоступность информационных ресурсов;

– проникновения вредоносного кода в программное обеспечение технических средств АКС;

– утечки информации с ограниченным доступом, обрабатываемой в АКС, за пределы периметра системы.

Таким образом, можно отметить следующие особенности при организации защиты периметра автоматизированных картографических систем:

– необходимость подключения АКС к сетям общего пользования;

– необходимость контроля двунаправленного потока информации(извне и в систему) по всем физическим каналам, имеющим выход за пределы контролируемой зоны;

– необходимость применения организационных и технических мер защиты информации, исключающих неправомерное применение внешних накопителей информации.

В настоящее время нормативно-методические документы (НМД) для проведения контроля эффективности проведенных мероприятий по защите периметра не в полной мере отвечают специфике защиты информации в АКС.

Для решения этой задачи в ЗАО «АСИС» разработана методика контроля эффективности мероприятий по защите периметра АКС, позволяющая компенсировать недостаточную полноту существующей НМД.

Марков А.С., Фадин А.А., Цирлов В.Л., Рауткин Ю.В.
Россия, Москва, ЗАО «НПО «Эшелон»

О ЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

В настоящее время основной тенденцией построения систем защиты информации является комплексный подход. Инфраструктура крупных организаций становится настолько многоуровневой и в целом сложной, что уследить за огромным потоком сведений о нарушениях информационной безопасности и оценить значимость каждого из них бывает чрезвычайно сложно. Это приводит к росту требований к квалификации и качеству работы персонала автоматизированной системы. Решение обозначенных выше проблем появилось почти 10 лет назад, но особенно востребованным оно стало только в последние годы.

SIEM представляет собой распределенную систему, включающую в себя сервер, выполняющий основные работы по агрегации и корреляции событий, и сенсоры, собирающие информацию, передаваемую из различных компонентов АС. В крупных системах отдельным модулем иногда реализуют компонент хранения журналов событий, как правило, на базе быстрых систем хранения данных. Наиболее популярными протоколами передачи журнальных данных являются Syslog, FTP, ODBC и SNMP. Кроме того, важно не только поддерживать транспортный протокол, но и

распознавать формат и семантику содержимого журнала. Для этих целей имеются форматы Syslog, CLF, SCAP, CIM и CEF, предлагаемые для его использования различными поставщиками продуктов в области безопасности.

Рассмотрим компоненты типовой архитектуры SIEM на примере программного комплекса «KOMRAD Enterprise SIEM» производства ЗАО «НПО «Эшелон». Рассматриваемое решение содержит:

– источники событий - объекты ИТ-инфраструктуры (конечные устройства и системы, такие как серверы, активное сетевое оборудование, базы данных, средства защиты информации), мониторинг безопасности которых является основной задачей «KOMRAD Enterprise SIEM»;

– журналы событий объектов ИТ-инфраструктуры;

– средства сбора и передачи информации - агенты, собственные средства конечных устройств и систем или запросы от сенсора, передающие данные о событиях ИБ от источников событий в ядро системы;

– rsyslog - средство приёма данных о событиях ИБ и их агрегации в журналах;

– журналы данных о событиях информационной безопасности, поступивших от конечных устройств и систем;

– плагин - набор инструкций, в соответствии с которыми сенсор обрабатывает данные из журналов;

– сенсор - программный модуль, нормализующий и передающий данные в базу данных (БД) «KOMRAD Enterprise SIEM»;

– база данных, в которой хранятся архивы событий ИБ, данные об инцидентах ИБ и информация о настройках системы;

– модуль корреляции - модуль анализа данных, с помощью которого выявляются инциденты ИБ;

– веб-интерфейс -средство взаимодействия администратора безопасности с системой;

– ядро - совокупность программных модулей «KOMRAD Enterprise SIEM».

При возникновении событий ИБ на конечных устройствах или системах данные об этом записываются в журналы состояния соответствующих объектов ИТ-инфраструктуры и в режиме времени, близком к реальному, отправляются на сервер «KOMRAD Enterprise SIEM» агентами, собственными средствами конечных устройств и систем или по запросу от сенсора к БД (MySQL, MSSQL).

Сервер «KOMRAD Enterprise SIEM» принимает данные, агрегирует и записывает их в журналы в соответствии с типом источника событий с помощью утилиты rsyslog. Сенсор обрабатывает журналы в соответствии с логикой плагинов, обеспечивающих поддержку работы с конечными устройствами и системами различных типов, после чего нормализованные данные поступают в БД «KOMRAD Enterprise SIEM», где каждому событию ИБ присваивается уникальный персональный идентификатор. После этого выполняется обработка данных модулем корреляции в соответствии с заранее определёнными правилами корреляции и политиками, на основании которых выявляются инциденты ИБ.

Дальнейшей рост эффективности систем безопасности связан, прежде всего, с качеством их взаимной интеграции, одним из столпов этого объединения являются SIEM-системы, решающие различные задачи поддержки процессов управления, как безопасностью, так и всей IT-инфраструктурой предприятия.

Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

К ВОПРОСУ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЪЮТЕРНОЙ ИНФОРМАЦИИ

Если еще десять лет назад считалось, что преступления в сфере компьютерной информации и высоких технологий в России явление относительно редкое, то в настоящее время доля такого рода преступных деяний, в том числе и посредством сети Интернет, существенно увеличилась.

По заказу Агентства передовых оборонных исследовательских проектов Министерства обороны США (AdvancedResearchAgency – ARPA) в 1969г. Калифорнийский университет в Лос-Анджелесе, Стэнфордский исследовательский центр, Университет штата Юта и Университет штата Калифорния создали экспериментальную сеть передачи пакетов информации, названную Arpanet, которая в рамках проекта объединила эти 4 учреждения. в1983 г. из Arpanet выделилась сеть Milnet, использовавшаяся только в интересах Министерства обороны США. В 1983 году Arpanet, перешла на протоколы передачи данных TCP/IP, использование которых позволяет устанавливать и поддерживать виртуальный канал (т.е. логическое соединение), и осуществлять передачу информации между компьютерными сетями разной архитектуры и топологии. Именно благодаря протоколу TCP/IP был создан Интернет – глобальная компьютерная сеть, охватывающая весь мир, состоящая в настоящее время из многих тысяч корпоративных, научных, правительственных и

домашних компьютерных сетей, используемая как средство общения, обмена информацией, рынка услуг, финансовых отношений, моментального производства платежей по всему миру.

В настоящее время Интернет доступен не только через компьютерные сети, но и через спутники связи, радиосигнал, кабельное телевидение, телефон, сотовую связь, специальные оптико-волоконные линии и электропровода. Интернет имеет около 50 миллионов пользователей в более чем 150 странах мира, ежемесячно размер сети увеличивается на 7-10%. По сообщениям СМИ Россия в 2013-2014 году заняла первое место в мире по росту пользователей сети Интернет. Растет и криминогенный потенциал «всемирной паутины»: в сущности, посредством эксплуатации возможностей сети, могут совершаться самые разнообразные преступления (хищения, подделка данных и др.), а деяний, совершение которых с помощью Интернет невозможно, становится все меньше.

Количество преступлений в сфере компьютерной информации стремительно растет по мере развития технологий, телекоммуникационных сетей и увеличения числа персональных компьютеров. Если в 1997 году в стране было зарегистрировано 7 преступлений, предусмотренных ст. 272 УК РФ, то в 2012 году - 2820, а в 2013 – 2563 преступлений в сфере компьютерной информации. При этом, указанные данные не в полной мере отражают истинное положения положение. Компьютерные преступления отличаются высокой латентностью, сложны в выявлении и раскрытии. Доказательства по ним могут быть уничтожены в считанные секунды, а идентифицировать компьютер, с помощью которого осуществлен неправомерный доступ, бывает сложно. Не все потерпевшие (особенно частные, коммерческие структуры), выявив преступное посягательство, обращаются в правоохранительные органы. Это происходит по разным причинам – из-за боязни раскрыть свои технические и коммерческие секреты, обнародовать ненадежность информационной защиты, а порой и опасение выявления собственных финансовых махинаций.

Компьютерные технологии все чаще становятся средством для совершения традиционных преступлений: против собственности, в сфере экономики, против конституционных прав и свобод человека и гражданина и т.д. Однако, как показывает практика, следователи нередко такие преступления квалифицируют только по статьям уголовного кодекса, предусматривающим ответственность за традиционное преступление, игнорируя совершение этих преступлений с использованием компьютерных технологий. Это приводит к искажению статистических данных о количестве совершаемых в России преступлений в сфере компьютерной информации.

В последнее десятилетие появилась статистика совершения преступлений, связанных с использованием глобальной сети Интернет.Так, по данным Управления «К» МВД России Интернет-мошенничества являются самыми распространенными преступлениями в сети, и их число неуклонно растет – за 6 месяцев 2012 года зафиксировано 1443 таких преступления. Число преступлений, совершаемых посредством сети Интернет, растет пропорционально числу пользователей сети. Компьютерная техника и глобальные сети позволяют преступникам действовать анонимно, не оставляя своих данных и примет, совершать преступления с территории иных государств, а также действовать совместно с соучастниками из других стран.

Специфика преступлений в сфере компьютерной информации и высоких технологий обусловлена использованием при их совершении различных новейших достижений мировой науки и техники, необходимостью обладания определенным уровнем специальных познаний и наличием специального инструментария, что с учетом высокой латентности подобных общественно-опасных деяний затрудняет их выявление и фиксацию, а также организацию противодействия им, включая их пресечение и предупреждение. Все это требует от сотрудников правоохранительных органов высокого уровня профессиональной подготовки для борьбы с преступлениями в сфере компьютерной информации и высоких технологий.

Ныркov А.П., Черняков А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

АЛГОРИТМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

Причины, по которым происходит потеря данных, разнообразны. Достаточно частая причина – отказ оборудования в связи с механическими или электрическими повреждениями, ошибками контроллеров систем хранения данных - 44% случаев. Каждый третий случай связан с человеческим фактором (случайное удаление, неправильная эксплуатация систем хранения данных) – 32%. Ошибки программного обеспечения при работе с файлами, при резервном копировании и восстановлении составляют 14% от общего числа случаев потери данных. Вопреки распространённому мнению, компьютерные вирусы являются причиной утраты информации лишь в 7% случаев, а на долю стихийных бедствий приходится и того меньше – 3%.

Наиболее надёжным способом защиты информации от порчи или утраты является резервное копирование. Идея этого метода проста – данные, находящиеся в вычислительной системе, копируются на независимый носитель или дисковую систему, сохраняя своё состояние на

определенный момент времени с целью восстановления в случае повреждения или утраты оригинала.

Для организации надежной системы резервного копирования требуется составить перечень информационных ресурсов, подлежащих защите, расставить приоритеты критичной информации, задать время хранения и частоту создания копий, определить меры безопасности по пресечению неавторизированного доступа, рассчитать необходимый размер репозитория для долгосрочного и оперативного хранения информации.

Для сокращения объема репозитория применяют различные алгоритмы резервного копирования. Наибольшей популярностью пользуются полное, инкрементное и дифференциальное резервирование. Эти алгоритмы могут применяться как по отдельности, так и вместе. Кроме того, во избежание многократного сохранения одних и тех же данных, применяют метод дедупликации, заключающийся в исключении из резервной копии повторяющихся блоков данных и заменой их на ссылки.

Проведенные исследования показывают, что алгоритм полного копирования создает большое количество дублируемой информации. В результате объём репозитория растет очень быстро. Дифференциальный подход показывает хороший результат на коротких промежутках, начиная с 0,1 объёма полной резервной копии, но уже к концу 14-го дня дифференциальная копия составляет ~0,5 от полной. Инкрементный алгоритм является наилучшим с точки зрения экономии ресурсов, однако легко показать, что он обладает более низкой надёжностью по сравнению с вышеуказанными. Из-за отсутствия избыточности данных при утрате одной копии в цепочке их восстановление становится невозможным. Использование всех трех алгоритмов в многоуровневой схеме показывает хороший результат по времени копирования и требуемому объёму. Недостатком является неравномерное использование системы резервного копирования – при переходе на «нижний» уровень, количество копируемых данных возрастает по отношению к верхним уровням.

Яковлев А.Е.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПЕРЕХВАТ АУДИОИНФОРМАЦИИ С ПОМОЩЬЮ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ КАК ОДИН ИЗ ЭФФЕКТИВНЫХ ПУТЕЙ НЕГЛАСНОГО ПОЛУЧЕНИЯ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ

Ценность информации с каждым годом всё возрастает. В современном мире люди пытаются узнать секреты других людей – будь это информация о новейших научно-технических разработках, информация о состоянии дел человека (организации), банковская или медицинская тайна. За многовековой период накопилось огромное количество способов сбора информации о конкурентах или противниках. Далее рассмотрим основные способы сбора информации (ведения разведки), их три:

– на основе открытых источников (презентации, публикации в СМИ, официальные отчеты, рекламные материалы);

– через людей - носителей информации (переманивание, подкуп, шантаж, вербовка);

– через технические каналы (закладные устройства, компьютерные вирусы, копирование документов, просмотр почты).

Для получения и анализа информации из открытых источников необходима мощная аналитическая служба, также велика вероятность дезинформации. Но огромным плюсом данного способа является его полная законность. Люди, как канал утечки, очень уязвимы. Вербовкой занимаются с давних времен и накоплен огромный опыт.

Для того, чтобы получить нужную информацию через технические каналы, необходимо одновременное выполнение трёх условий:

– наличие опасного сигнала;

– наличие среды распространения;

– наличия технического средства приёма сигнала.

Очень эффективным способом добывания ценной информации через технические каналы является съем аудио сигнала. Чаще всего для этого используют так называемые закладные устройства (сокр. З.У.), которые могут быть установлены в линии связи или в помещения, где циркулирует конфиденциальная информация. В целом такие устройства можно классифицировать:

– по каналу передачи информации (радио и ИК-закладки, с записью на носитель информации, с передачей по токопроводящим линиям);

– по способу восприятия информации (микрофонный тип, вибрационный, с подключением через коммуникационные линии);

– по наличию устройства управления (с непрерывным излучением, с дистанционным управлением, с автоматическим включением при появлении сигнала);

– по внешнему виду (обычный или камуфлированный вид);

– по используемому источнику питания (с источником питания и без).

Самым распространённым видом З.У. являются радиозакладки. Они получили широкое распространение благодаря своим достоинствам, таким как простота установки, возможность шифрования передаваемой информации, возможность слежения за мобильными объектами на больших расстояниях. Но радиозакладки не лишены недостатков: фиксированный радиус действия закладки, ограничение по времени работы, возможность перехвата передаваемой информации. Классификация радиозакладок:

– по принципу формирования сигнала (активные, полуактивные, пассивные);

– по способу закрытия передаваемого сигнала (без закрытия, сложные виды модуляции, кодирование);

– по дальности действия (малой, средней, большой дальности).

Технологии не стоят на месте и технические средства добывания информации, в т.ч. радиозакладные устройства, совершенствуются с каждым годом: линейные размеры уменьшаются, улучшается маскировка, увеличивается время их работы и растет радиус действия. Известны и методы защиты от таких устройств – поиск З.У. как физического объекта (визуальный осмотр, контроль с помощью видеонаблюдения, применение металло-детекторов), поиск З.У. как электронных средств (использование индикаторов поля, применение специальных приемников, использование нелинейных локаторов).Необходимо не зацикливаться на одних лишь технических моментах защиты конфиденциальной информации, а подходить к этому вопросу комплексно, используя правовые, морально-этические, организационные и технические способы предотвращения утечки информации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

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

ОРГАНИЗАЦИЯМЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Организация менеджмента инцидентов информационной безопасности(ИБ) в автоматизированных системах специального назначения (АССН) является актуальной задачейв условиях постоянновозникающих новых угроз ИБ,характерных для информационного противостояния. Недостаточно высокий уровень организации системы защиты информации (СЗИ),обусловленной разобщённостью процессов,требует решения следующих задач:

– обнаружение, регистрация и оповещение об инцидентах информационной безопасности иихэкспертная оценка;

– реагированиена различныенесанкционированные воздействия на информацию в АССН, включая порядок применения защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий;

– ведение базы со статистическими данными об инцидентах ИБ для проведения глубокого аналитического анализа с целью своевременного принятия защитных мер и улучшению общего подхода к созданию эффективной СЗИ в АССН.

Основным путем решения данных задач является внедрения системы менеджмента инцидентов ИБ в АССН.

В соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007«Менеджмент инцидентов информационной безопасности»необходимо выполнить рядорганизационных мероприятий, включающих в себя формулирование и разработку политики менеджмента инцидентов ИБ, а также документальное отображение самой системы менеджмента инцидентовИБ с выходом соответствующего ведомственного нормативного акта.

Системаменеджмента инцидентов ИБ должна быть предназначена для всех сотрудников,имеющих авторизованный доступ к информационным ресурсам АССН иместам их расположения. В ней необходимо осветить вопросы значимости системы менеджмента инцидентов ИБ, общее представление об угрозах ИБ и алгоритм действий должностного лица при обнаружении нового инцидента ИБ.На данном этапе с сотрудниками также необходимо провести цикл занятий посвящённых основам ИБ.

Система менеджмента инцидентовИБ должна содержать такие элементы, как: классификацию инцидентовИБ по «значимости», обязанности и распределение функций ответственных лиц по видам деятельности, механизм анализа обнаруженных событий ИБ и варианты дальнейшего реагирования на инциденты ИБ.

На последующем этапе эксплуатации системы менеджмента инцидентов ИБособое место займут вопросы обобщения накопленного опыта и определение методов повышения безопасности.

В конечном итоге рассмотренные выше мероприятия позволят повысить эффективность СЗИ в АССН, в первую очередь за счёт снижения вероятности реализации угроз целостности, доступности и конфиденциальности.

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

МЕТОДЫ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ УПРАВЛЕНИЯ ЗАЩИЩЁННЫМИ МУЛЬТИСЕРВИСНЫМИ СЕТЯМИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ НЕЧЁТКОГО ВЫВОДА

Системообразующей основой ведомственной инфокоммуникационных сетей связи (ИКСС) является защищенная мультисервисная сеть специального назначения (ЗМС СН), которая создается на основе единой сетевой инфраструктуры и представляет собой цифровую телекоммуникационную сеть интегрального обслуживания с набором служб, обеспечивающих перенос разнородного трафика

с заданными количественными и качественными характеристиками предоставления пользователям инфокоммуникационных услуг.

В данной работе показано, что иерархия управленческих задач ЗМС СН представляет собой как вертикальные связи, так и горизонтальные связи в рамках как одного уровня, так и между уровнями управления пирамиды TMN (TelecommunicationsManagementNetwork – сеть управления электросвязью). Показано также, что оперативное оптимальное управление затрудняется вследствие больших размерностей совокупности решаемых оптимизационных задач, которые обеспечивают решение управленческих задач. Обосновывается, что многообразие, разнородность, неполнота, неточность и нечеткость исходных данных, обрабатываемых и учитываемых в задачах управления ЗМС СНпредопределяют необходимость использования средств и методов искусственного интеллекта (ИИ) при их решении. Для обеспечения оперативности и достоверности принимаемых управленческих решений в работах показана целесообразность применения технологии интеллектуальных мультиагентов (ИМА).

Учитывая разноплановость, многокритериальность, большую размерность решаемых задач по управлению ЗМС СН, часть процедур управления предлагается реализовывать на основе технологии интеллектуальных агентов (ИА), основой которых является технология «агент-менеджер».Основными свойствами ИА являются:

1. Адаптация. Агенты системы адаптируются к сетевой архитектуре и адекватно отвечают на изменения в конфигурации сетевого оборудования.

2. Рациональность распределения ресурсов. Элементы ИА равномерно распределены по всему периметру ЗМС СН, что позволяет рационально (оптимально) распределить вычислительные ресурсы.

3. Отказоустойчивость. Нет выделенного центра управления (центра принятий решений), так как агенты распределены по всей системе.

4. Возможность централизованного управления.

Координацию оптимизационных задач предлагается реализовывать на основе методов нечётких когнитивных карт. Рассматривается следующая совокупность оптимизационных задач:

– управления ресурсами ЗМС СН (распределение потоков, управление пропускными способностями каналов связи);

– управление процедурами маршрутизации (с учётом приоритезации трафика);

– управление рисками угроз информационной безопасности ЗМС СН;

– управление устойчивостью ЗМС СН (управление надёжностью (аппаратно-программной, структурной) и живучестью ЗМС СН, управление процедурами обеспечения помехоустойчивости в данной работе не рассматривается).

Также рассматривается задача оперативного оценивания параметров трафика ЗМС СН.

Общая структура оптимизационных задач представляется в виде задач математического программирования с чёткими целевыми функциями и набором нечётких ограничений. Координирующие воздействия формируются в виде функций изменений значений носителей нечётких множеств ограничений оптимизационных задач, а также изменений их функций принадлежности.

Проведён анализ применения нечётких ситуационных сетей для управления устойчивостью ЗМС СН, который показал эффективность его применения при многошаговых процедурах управления.

Полученные в работе результаты позволили снизить время цикла управления приблизительно на 8-17% при сохранении параметров качества связи.

Аксенов С.С., Лощенин Д.Е.,Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

К ВОПРОСУ ОБ АНАЛИЗЕ ЗАЩИЩЕННОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

Для обеспечения надежной защиты операционных систем, необходимо постоянно анализировать всевозможные источники угроз, сопоставлять им уязвимости и определять потенциальные угрозы, реализация которых прямо или косвенно может нанести вред операционной системе (ОС). Одной из наиболее распространенных операционных систем, является операционная система Linux.

Сегодня многие организации остановили свой выбор на ОС Linux, взяв ее на вооружение в качестве основной платформы. Причем, если раньше эта ОС использовалась преимущественно в качестве основы для построения недорогих маршрутизаторов, Web- и почтовых серверов, то сегодня имеется целый ряд более серьезных задач, которые удобно решать на ее базе: серверы баз данных и доступа, серверы приложений и полнофункциональные межсетевые экраны. Благодаря высокой устойчивости ОС Linux ей можно смело поручать длительные вычислительные задачи.

В качестве примера решения проблемы с организацией защиты в ОС предлагается рассмотреть модель управления доступом RSBAC (Rule Set Based Access Control), позволяющую построить защищенную систему на базе ядра ОС Linux.RSBAC - это надстройка над ядром Linux и комплект утилит управления, позволяющие создать на базе любого дистрибутива Linux защищенную систему. Поскольку в России имеется своя система сертификации, для нас более интересно рассмотреть предоставляемые системой RSBAC механизмы обеспечения безопасности. Реализация этих механизмов выполнена на уровне ядра системы и позволяет эффективно контролировать все процессы. Системные вызовы, затрагивающие безопасность, дополняются специальным кодом, выполняющим обращение к центральному компоненту RSBAC. Это компонент принимает решение о допустимости данного системного вызова на основе многих параметров: типа запрашиваемого доступа (чтение, запись, исполнение); субъекта доступа; атрибутов субъекта доступа; объекта доступа; атрибутов объекта доступа.

Функционально RSBAC состоит из нескольких модулей, а центральный компонент принимает комплексное решение, основываясь на результатах, возвращаемых каждым из активных в данный момент модулей. Вся дополнительная информация, используемая RSBAC, хранится в дополнительном каталоге, который доступен только ядру системы. В зависимости от описанного уровня абстракции исполняемых задач и необходимой степени защиты выбираются различные сочетания модулей. RSBAC дает возможность избавить систему от общих недостатков ОС семейства UNIX. Появление категории "офицер безопасности решает проблему не подконтрольности основного администратора системы, а категории "офицер по защите данных децентрализует администрирование, позволяя практически реализовать принцип "четырех глаз", в соответствии с которым все критичные операции не должны производиться в одиночку.

Действительно, возможно построение системы, в которой нового пользователя по-прежнему заводит root, однако его уровень безопасности и права доступа к ресурсам задаются security officer и data protection officer. RSBAC можно интегрировать с любым дистрибутивом Linux, необходимо лишь внести соответствующие исправления в исходные тексты ядра системы. Эта процедура осуществляется при помощи стандартной утилиты patch и прилагаемого "файла-заплатки", который предлагается для разных версий ядра. После этого происходит его обычная настройка, при этом в настройке появляется несколько новых пунктов. После загрузки ядра настройка системы производится при помощи прилагаемых утилит администрирования. Система снабжена подробной документацией и подборкой теоретических материалов, где описаны все используемые модели защиты.

Таким образом, применение Linux в сочетании с RSBAC позволяет строить защищенные автоматизированные системы, в том числе и для силовых структур.

Аксенов С.С., Гурьев С.Н., Кочкин В.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В ЛВС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящее время при реформировании ВС РФ локальные вычислительные сети специального назначения (ЛВС СН) обеспечивают информационные процессы в автоматизированных системах военного назначения (АС ВН). Исходя из этого, одним из важных направлений повышения эффективности управления войсками и связью является совершенствование методов и средств защиты информации в ЛВС СН. Постоянное структурное и функциональное усложнение средств обработки информации способствует появлению современных технологий цифровой обработки информации и новых уязвимостей. Этим создается множество вопросов защиты информации в ЛВС СН и расширяется спектр угроз безопасности информации. В качестве источника не преднамеренной угрозы и основных нарушителей в ЛВС СН рассматриваются санкционированные пользователи, имеющие регламентированный доступ к сетевым ресурсам, знакомые со структурой и принципами построения ЛВС СН, спецификой решаемых задач и возможностью полнодоступного использования штатных средств вычислительной сети.

Одним из основных элементов ЛВС СН является управляемый коммутатор. Коммутатор позволяет построить ВЛВС на основе портов и поддерживать управление через web браузер. Возможности управляемого коммутатора позволяют логически разделять сеть на сегменты. При этом сетевые устройства, подключенные к группе портов (определяются настройками коммутатора), выделяются в виртуальную сеть. Так же имеется возможность включить одновременно несколько портов в одну группу ВЛВС. Это логически изолирует группы физических портов и обеспечивает передачу трафика с нескольких виртуальных сетей в один или несколько физических портов. Количество ВЛВС будет зависеть от решаемых оперативно-тактических задач, либо от вида оперативного мероприятия, проводимого в штабе.

Целесообразность использования в ЛВС СН виртуальных локальных вычислительных сетей обусловлена тем, что одновременно решаются следующие задачи:

1. Повышается производительность в каждой из виртуальных сетей за счет того, что управляемый коммутатор передает пакеты сообщений только узлу назначения.

2. Повышается безопасность сети вследствие изоляции прав доступа пользователей к другим виртуальным сетям и создания защитных барьеров на пути широковещательных штормов.

3. Уменьшается нагрузка на администратора ЛВС при перемещении пользователей.

Таким образом, построение виртуальных локальных вычислительных сетей в ЛВС СН позволяет повысить безопасность, производительность сети и пропускную способность общей локальной сети, уменьшить рутинный труд обслуживающего персонала ЛВС.

Алашеев В.В.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

СИСТЕМНЫЙ ПОДХОД ВЫБОРА УГРОЗЫ СЪЕМА ИНФОРМАЦИИ

Формирование и выбор угроз съема информации нарушителем на объекте информатизации наиболее рационально проводить на основе системного подхода метода анализа иерархий (МАИ). В этом методе предусматривается декомпозиция проблемы на части, ее структурирование и выделение иерархии, содержащей различные главные цели, подцели, уровней мероприятий, альтернатив, подлежащих оценке и дальнейшая обработка последовательности суждений по попарным сравнениям. Данный метод включает процедуры синтеза множественных суждений, оценку приоритетности факторов и нахождения альтернативных стратегий (решений). Преимуществом МАИ над большинством существующих методов оценивания стратегических альтернатив является четкое выражение суждений экспертов и лиц, принимающих решения, а также ясное представление структуры проблемы: элементов и взаимозависимостей между ними. Метод анализа иерархий опирается на достаточно простые элементы, которые оцениваются в шкале МАИ в виде суждений экспертов. А затем на основании обработки экспертных оценок определяется относительная степень их взаимного влияния в иерархии.

Результатом исследования являются вероятности выбора эффективных угроз по съему информации, значения которых применяются для расчета выбора альтернатив по осуществлению угроз по добыванию информации.

Задача определения вероятности выбора наиболее эффективных альтернатив со стороны нарушителя рассматривается с целью построения модели действий нарушителя в процессе реализации угроз.

Указанная цель достигается за счет реализации угроз, имеющих своей целью негласное добывание информации, циркулирующей на объектах информатизации военного назначения (ОИ ВН). Предполагается, что нарушитель обладает некоторыми сведениями о ОИ, полученными в результате технической разведки. Это может быть сведения о применяемых средствах защиты и имеющихся уязвимостях ОИ.

Для исследования действий нарушителя в процессе реализации угроз составляется матрица парных сравнений.

При составлении матрицы попарных сравнений использована шкала относительной важности объектов (1-9), где 1- равная важность, 3- умеренное (незначительное) превосходство одного над другим, 5 - существенное или сильное превосходство одного над другим, 7 - очень сильное превосходство, 9 - абсолютное превосходство. 2, 4, 6, 8 — промежуточные оценки между соседними суждениями. Обратные величины применяются к элементам, которые менее значимы при парных сравнениях.

Сравнивая полученные значения приоритетов, определяют рейтинг для всех стратегий. Высокий рейтинг будет соответствовать наибольшему значению глобального вектора приоритета или наиболее предпочтительной альтернативной стратегии.

После проведения расчетов выбирается максимальный элемент полученного вектора приоритетов, который является показателем того, что альтернатива является наиболее приемлемой для реализации поставленной цели.

Таким образом, полученные результаты позволяют определить значения вероятностей выбора i-ой угрозы, реализуемой с целью негласного добывания информации, и могут быть использованы для расчета времени, необходимого нарушителю для организации подготовительного этапа съема информации на ОИ ВН.

Анисимов В.В., Стародубцев Ю.И., Чукариков А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ПРЕВЕНТИВНОЙ ЗАЩИТЫ ИТКС СН, ИСПОЛЬЮЗУЮЩЕЙ РЕСУРСЫ ЕСЭ РФ

В настоящее время сложилась ситуация, когда силы и средства связи в основе своей являются стационарными, основная задача которых организация сети доступа. При этом определено, что

транспортной основой ИТКС СН является Единая сеть электросвязи РФ (ЕСЭ РФ), которая предоставляет необходимые пропускные способности в её интересах.

Отличительной особенностью современности в области информационных технологий является развитие общемирового единого информационно-телекоммуникационного пространства (ОМЕИТП), где ЕСЭ РФ представляет собой сегмент, подключённый к нему и условно ограниченный государственной границей. Значит, можно считать, что и ИТКС СН является частью ОМЕИТП.

Становится очевидным тот факт, что чем больше ИТКС интегрировано в ОМЕИТП, тем большее число КСВ она испытывает. Вместе с интеграцией в ОМЕИТП происходит распределение объекта защиты по ОМЕИТП.

Превентивная защита создаёт такие внешние условия функционирования ИТКС, что при любом рациональном изменении регулируемых параметров ИТКС, состояние ИТКС не выйдет из области допустимых состояний в определённом промежутке времени.

При использовании ресурсов ОМЕИТП, все эти ресурсы являются общими для всех СУВ, их использующие. Соответственно, для другой СУВ деление на области допустимых и критических состояний будет другим. Необходимо определить (предположить), как всё множество состояний объекта делиться для каждой СУВ. После этого соотнести полученные деления, выявить какие состояния являются «хорошими» для всех, а какие «плохими» для всех. Именно это не позволит избежать конфликта и ввести элемент обсуждения и договора между СУВ. Также, зная, какие состояния объекта являются для всех субъектов «плохими», можно экономить ресурсы управления, так как система управления другого субъекта также будет выводить объект из этого состояния.

При этом стоит понимать, что ведущая роль принадлежит системе связи по отношению к системе противника. Имея возможность изменять систему связи по любому, случайному сценарию за самое малое время, система разведки противника не сможет собрать объективную информацию о нашей СУВ и предоставить её для принятия решения. Это идеальное представление, но эта возможность всегда ограниченна определённым ресурсом.

Анистратов И.В., Калюка В.И., Мешков И.С., Овсянников С.Н.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
Санкт-Петербург Военная академия связи имени Маршала Советского Союза С.М. Буденного, войсковая часть 25522

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА WiMAX В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В современных условиях высокоразвитых инфотелекоммуникационных технологий возникает объективная необходимость комплексной оценки уязвимостей сетей широкополосного радиодоступа (СШРД) WiMAX, позволяющей заблаговременно анализировать возможные риски прослушивания, модификации и подмены информации и проводить комплекс мероприятий по защите информации. Основными целями защиты информации в СШРД WiMAX являются:

обеспечение необходимого уровня защищенности от внешних и внутренних угроз и создание условий сохранения секретности и конфиденциальности информации.

Цели позволяют сформулировать задачи защиты информации в СШРД WiMAX:обнаружение и мониторинг внутренних и внешних угроз информационной безопасности;совершенствование и стандартизация применяемых методов и средств защиты информации.

Каждая инфотелекоммуникационная система по-своему индивидуальна. Поэтому и комплексная оценка СШРД WiMAX нацелена на выявление возможных факторов, влияющих на уязвимость информации, подлежащей защите именно в этих сетях. Для этого необходимо построить модель угроз информационной безопасности СШРД WiMAX и выявить каналы утечки, опираясь на комплексную оценку уязвимостей в условиях неопределенности, когда результаты принимаемых решений по устранению «слабых мест» неизвестны. Обоснование принимаемых решений в условиях неопределённости (априорной) возможно путем построением алгоритмов адаптивного управления.

В СШРД WiMAXоднойизглавныхзадачявляетсяобеспечениезащитыинформации, гдеканалпередачиданныхчасторазделяетсямеждубольшимколичествомпользователей и является общедоступным.Именнопоэтимпричинампризработкестандарта IEEE 802.16e-2005, 2009 подуровнюбезопасностиуделялосьособоевнимание.

С одной стороны, удовлетворяетребованиям (NSP, network service provider), подуровеньбезопасностиобеспечиваетуслугиаутентификациииавторизации. Сдругойстороны, подуровеньбезопасностистандарта IEEE 802.16e-2005, 2009 удовлетворяетосновнымтребованиямпользователей – уверенностьвконфиденциальностиицелостностипередающихсявсетиданных, атакжевтом, чтоабонентвсегдасможетполучитьдоступксервисам.Подуровеньбезопасностиопределентольконакана льномуровнеэталонноймодели OSI. Поэтомувсепоставленныепереднимзадачирешаютсятремяспособами:

– использованиесредствпротокола EAP (extensible authentication protocol) иалгоритма RSA (rivest shamir iadleman) дляаутентификацииавторизации абонентских станций;

– осуществлениекриптографическихпреобразованийнадтрафиком, обеспечиваяконфиденциальность, целостностьиаутентичностьданных, атакжеаутентичностьицелостностьслужебныхсообщений MAC (media access control)-уровня;

– использованиепротоколауправленияключами PKM (privacy and key management protocol) длябезопасногораспределенияключевойинформации.

Уязвимости в стандарте IEEE 802.16:

– атаки физического уровня, такие как глушение передачи сигнала, ведущее к отказу доступа или лавинный наплыв кадров (flooding), имеющий целью истощить батарею станции;

– ложные несертифицированные базовые станции. В стандарте проявляется явная несимметричность в вопросах аутентификации. Предложенное решение этой проблемы – инфраструктура управления ключом в беспроводной среде (WKMI, wireless key management infrastructure), основанная на стандарте IEEE 802.11i. В этой инфраструктуре есть взаимная аутентификация с помощью сертификатов X.509;

– неслучайные генерации базовой станцией ключей авторизации. Взаимное участие базовой и абонентской станции в генерации полностью или частично решило бы эту проблему;

– возможность повторно использовать ключи TEK (traffic encryption key), чей срок использования уже истек.

Байбиков Г.Р., Пицун А.Л.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ТРЕНАЖЕРОВ В ПРОЦЕССЕ ИЗУЧЕНИЯ ПРОГРАММ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Информационные технологии стали неотъемлемой частью жизни современного общества. В связи с этим перед современной системой образования ставится сложная задача опережающей подготовки нового поколения к условиям существования и профессиональной деятельности в глобальном информационном обществе.Освоения практических навыков, предназначенных для обеспечения защиты передаваемой в сетях информации, а также для защиты локальных сетей от несанкционированного доступа, попыток взлома и нарушения их работоспособности, является одной из наиболее сложных задач в процессе обучения и подготовки специалистов. Благодаря бурному развитию компьютерной техники и информационных технологий появилась возможность решить эту задачу за счет применения мультимедийных тренажерных средств.Наибольшей популярностью пользуются так называемые «виртуальные тренажеры», созданные на базе персональных компьютеров, обеспечивающие некое подобие рабочего места и, хотя бы приблизительно воспроизводящие динамику изучаемого объекта.

В качестве преимуществ использования тренажеровможно отметить следующее:интенсификация обучения без потери качества усвоения материала;возможность проведения практических занятий фронтальным методом (все обучаемые одновременно выполняют одну работу), что существенно повышает эффективность этого вида обучения;возможность широкого изменения условий эксперимента;возможность моделирования и безопасного исследования экстремальных и аварийных режимов работы оборудования;возможность относительно легкой и быстрой модификации элементов изучаемого оборудования к новейшим промышленным образцам;обеспечивается существенное энергосбережение по сравнению с использованием реальных лабораторных стендов, экономия учебных площадей, снижение капитальных, эксплуатационных и других затрат.

Таким образом, использование виртуальных тренажеров в процессе обучения с различным уровнем подготовки ведет к повышению уровня их знаний, умений, навыков обучаемых. Помогает сделать процесс обучения не только менее трудоемким для преподавателей и наглядным для обучаемых, но и выводят их степень подготовленности на новый качественный уровень. Также современные тренажеры позволяют реализовать на их платформе развитую систему защиты информации, позволяющую идентифицировать и аутентифицировать пользователей, собирать статистику процесса обучения.

Банный Э.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

ТАЙНА ПЕРЕПИСКИ, ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ, ПОЧТОВЫХ, ТЕЛЕГРАФНЫХ И ИНЫХ СООБЩЕНИЙ

Право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений закреплено в ч. 2 ст. 23 Конституции РФ и относится к категории основных конституционных прав и свобод человека и гражданина.Также рассматриваемое право на тайну

переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений закреплено в п. 1 ст. 8 Конвенции о защите прав человека и основных свобод, где говорится: «Каждый человек имеет право на уважение его корреспонденции».

Одной из основных гарантий права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений является общая конституционная обязанность государства, которая состоит в признании, соблюдении и защите прав и свобод (ч.2 Конституции РФ). Во исполнение данного конституционного положения приняты Федеральный закон от 17 июля 1999 г. «О почтовой связи» и Федеральный закон от 7 июля 2003 г. «О связи».

В названных федеральных законах закрепляется основная обязанность операторов связи по обеспечению права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Запрет нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений распространяется не только на операторов почтовой и иных видов связи, лиц, ведущих расследование уголовных дел и осуществляющих оперативно - розыскную деятельность, но и на всех остальных граждан.

Принцип обеспечения права на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений не перестает действовать с момента ограничения этого права на основании судебного решения . УПК РФ обеспечивает сохранение в тайне полученных сведений на протяжении всего производства по уголовному делу.В открытом судебном заседании переписка, запись телефонных и иных переговоров, телеграфные, почтовые и иные отправления могут оглашаться только с согласия лиц, являющихся адресатами (отправителями или получателями) этой корреспонденции. В противном случае указанные материалы оглашаются только при удалении публики из зала суда.

Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимально автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень ее защиты.

Анализ рассмотренных проблем показывает необходимость комплексного использования организационных мероприятий и применения специализированных программно-технических средств для обеспечения надежной защиты информации от несанкционированного доступа в системах управления военного назначения.

Бардюков Д.А., Подчасов О.П., Чернов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ СООБЩЕНИЙ ИСТОЧНИКОВ ВИДЕОИНФОРМАЦИИ НА ОСНОВЕПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТЫХ КАНАЛОВСВЯЗИ

В настоящее время наиболее распространенным, но наименее стойким является метод замены наименьших значащих битов или LSB-метод. Он заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях и видеофайлах. Данная погрешность равна наименьшему значащему разряду числа, определяющему величину цветовой составляющей элемента изображения (пикселя). Поэтому модификация младших битов в большинстве случаев не вызывает значительной трансформации изображения и не обнаруживается визуально. Другим популярным методом встраивания сообщений является использование особенностей форматов данных, использующих сжатие с потерей данных (например JPEG). Этот метод (в отличии от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения. Недостатками этих методов является низкая стойкость к ошибкам, это обусловлено тем, что при искажении только младших разрядов передаваемых информационных блоков полностью приводит к искажению встраиваемых сообщений. Другим недостатком данных алгоритмов является то, что объём встраиваемых сообщений намного меньше сообщения (т.е. контейнера).

Особенностью предлагаемого метода является то, что каждый бит открытой информации передаваемого блока в равной степени несёт информацию о каждом бите встраиваемой информации этого блока. Сущность метода заключается в том, что на передающем и приёмном сторонах генерируются псевдослучайные последовательности по числу встраиваемых сообщений. Затем на передающей стороне формируется такой информационный блок двоичной последовательности, который с одной стороны с требуемым качеством аппроксимирует открытое сообщение (контейнер), а с другой стороны в сумме с ранее с генерируемой псевдослучайной последовательностью (ПСП) с аналогичным качеством аппроксимирует соответствующее данным ПСП сообщение. На приёмной стороне получатель открытого сообщения (контейнера) принимает

сообщение с некоторыми искажениями, а остальные пользователи после наложения ПСП принимают соответствующие данным ПСП встраиваемые сообщения.

Результаты моделирования данного метода показали возможность встраивания от одного до трёх сообщений в одно открытое сообщение.

Борисенко К.А., Бекенева Я.А., Шоров А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственныйэлектротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

СИСТЕМА МОДЕЛИРОВАНИЯ ДЛЯ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ ТЕХНИК БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ОТ DDOS-АТАК

Веб–сайты правительств и правительственных организаций разных стран, а также ведущие IT-компании часто подвергаются массивным DDoS-атакам. Мировые лидеры по информационной безопасности выделяют обнаружение и защиту от DDoS–атак как главные задачи в своих исследованиях и разработках.

Для исследования DDoS атак и разработки новых механизмов защиты от них исследователи часто используют методы имитационного моделирования. Однако имитационное моделирование DDoS-атак часто несет проблемы, связанные с точностью имитации атак на уровне прикладных протоколов. Более того, в зависимости от установленного программного обеспечения на сервер, он может функционировать по-разному. В то же время создание крупных сетей в реальности часто требует больших затрат времени и ресурсов.

Поэтому мы предлагаем объединить методы имитационного моделирования и моделирования на реальных стендах. С помощью имитационного моделирования мы строим сеть атаки и объединяем ее с реальным сервером. Виртуальная сеть очень похожа на реальную сеть. Разработанный подход позволяет разрабатывать механизмы защиты, которые могут устанавливаться на различных участках сети атаки, а не только на входе у атакуемого сервера, как в случае с генераторами DDoS-трафика. Более того, защитные механизмы могут быть архитектурно зависимыми, что важно при проведении экспериментов максимально схожих с процессами в реальной сети. Важным достоинством является возможность подключения реальных узлов к виртуальной сети, что позволит увеличить точность экспериментов и позволит протестировать различные настройки и типы серверов.

Для разработки системы использовалась дискретно-событийная система моделирования OMNeT++. В качестве настроек сети, коммутации пакетов используется библиотека INET. В качестве настроек топологии была доработана библиотека ReaSE. Система имеет специальный сетевой интерфейс, который позволяет конвертировать трафик из виртуальной сети в реальную и обратно.

Созданная система позволяет быстро создавать новые топологии сети и легко настраивать ее компоненты, такие как серверы, маршрутизаторы, клиенты и др. Система позволяет моделировать поведение легитимных клиентов, различные сценарии атак, а также механизмы защиты. При реализации атак может быть задан целый ряд параметров отдельной атаки: используемый протокол, частота отправки пакетов, период выполнения атаки. Реализована возможность подмены адреса отправителя. Система спроектирована таким образом, что подготовка к проведению экспериментов требует малых временных затрат, что экономит время для создания и тестирования новых механизмов защиты. Кроме того, пользователь, проводящий эксперименты, не обязательно должен владеть навыками программирования.

Была успешно проведена верификация системы. Сравнение было выполнено между разработанной системой и сетями, построенными используя проект PlanetLab.

Авторы сделали множество экспериментов с различными сценариями DDoS–атак: TCP-Flooding атаки, HTTP атаки, ECHO атаки, Chargen атаки, NTP атаки. Эксперименты были выполнены без использования защитных методов и с фильтрующими методами (Ingress, Egress). Топология сети для проведения экспериментов состояла из 7 роутеров, 204 клиентов и 1 реального сервера. Задержки между узлами сети были равны 1 милисекунде.

Теперь приведем анализ экспериментов со сценарием атаки SYN–Flooding с использование метода Egress и без использования защитных методов. Во время SYN–Flooding атаки, 20% от всего количества клиентов (40 компьютеров) участвовали в атаке, SYN cookies были выключены на сервере для успешного проведения атаки. В начале атаки, на 10 секунде, количество использования сервера увеличивалось из-за все большего и большего количества клиентов, включающихся в атаку. До 15 секундой сервер успевал обрабатывать все запросы, но после TCP стек оказался переполнен и сервер не мог обрабатывать увеличивающееся количество запросов. С 15 секунды по 57 секунду сервер не мог отвечать на все приходящие SYN пакеты.

Были проведены эксперименты с использованием фильтров на 2, 3, 4 роутерах в виртуальной сети. В тоже время были клиенты, атакующие сервер, которые находились в локальной сети

роутера, который не использовал метод Egress Filtering. С увеличением количества фильтров мощность DDoS атаки уменьшалась.

Работа выполняется в рамках государственной работы «Организация проведения научных исследований» базовой части государственного задания Минобрнауки России, а также проектной части государственного задания Минобрнауки России (ЗАДАНИЕ № 2.136.2014/К).

Брунилин А.А., Куваев В.О., Петухов А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СЕМАНТИЧЕСКИЙ ПОДХОД ПРИ РЕШЕНИИ ОТДЕЛЬНЫХ ВОПРОСОВ РАЗГРАНИЧЕНИЯ ДОПУСКА ДОЛЖНОСТНЫХ ЛИЦ К ОБРАБОТКЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Разграничение допуска должностных лиц к обработке информации ограниченного доступа представляет собой многоэтапный процесс взаимодействия различных ведомств государственной организации. Взаимодействие имеет целью установить годность субъекта информационной деятельность для доступа к определённому классу информации. Порядок выполнения данных действий строго регламентирован и унифицирован для всех ведомств и организаций. Ряд этапов данного трудоёмкого процесса до настоящего момента не автоматизирован, не смотря на наличие такой возможности.

Например, не автоматизирован анализ исходных данных для классификации информации, обрабатываемой должностными лицами согласно номенклатуре должностей организации. Программное решение данной задачи могло бы повысить обоснованность решения руководителя организации на допуск сотрудника к обработке конкретного вида информации при сокращении времени и объёма рутинной работы должностных лиц режимного органа организации.

Также в настоящее время отсутствуют программные средства трансляции версий руководящих документов, определяющих степень секретности информации. Ввиду действия директивных указаний по немедленному уничтожению грифованных руководящих документов, утративших силу, и особенностей учёта фактов ознакомления должностных лиц с информацией ограниченного доступа, в ряде случаев установление степени осведомлённости и актуальности ограничения доступа к данным сведениям связано со значительными организационными сложностями и временными затратами.

Для решения обозначенных и ряда иных вопросов, связанных с разграничением допуска к информации ограниченного доступа, предлагается использовать семантический подход и онтологию как его программную реализацию.

Основой для решения может стать семантический анализ действующего перечня сведений ограниченного доступа и его проекция в программную онтологию. Подобный подход представляется наиболее рациональным, т.к. при построении семантической модели предметной области можно более гибко (по сравнению, например, с реляционной моделью) описывать множественные отношения принадлежности информационных сущностей классам (категориям). А аппарат логического вывода онтологий, основанный на EL-логике, позволяет однозначно и за конечное время классифицировать анализируемые информационные сущности по их семантическим признакам, что и представляет собой суть решения данной информационной задачи. Кроме того, возможности языка запросов к онтологиям SPARQL предоставляет возможности для решения более широкого круга последующих задач данного направления.

В статье предлагается концептуальный подход и основные шаги, направленные на решение описанных задач; раскрываются возможности и особенности применения программных онтологий для построения предметных областей задач, их преимущества применения онтологий по сравнению с реляционной моделью.

В заключении изложены выводы из проведённого исследования и перечислены основные направления работы для реализации семантического подхода при решении задач разграничения допуска должностных лиц к обработке информации ограниченного доступа.

Бударин Э.А., Гелметдинов М.И., Столяров А.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

МЕТОДИКА ОЦЕНКИ СТРАТЕГИИ РАСПРЕДЕЛЕНИЯ СРЕДСТВ РАДИОПОДАВЛЕНИЯ ПО ЭЛЕМЕНТАМ СИСТЕМЫ РАДИОСВЯЗИ

Ужесточающиеся требования к управлению ведомственными силами диктуют настоятельную необходимость всестороннего информационного обеспечения должностных лиц органов управления и предъявляют довольно жёсткие требования к ведомственной системе связи.

Анализ показывает, что ведомственные системы управления и связи функционируют в условиях непрерывного воздействия системы подавления, которая ведётся по определённым сценариям (стратегиям) с целью выбора наиболее эффективных способов воздействия (выбора

стратегии воздействия). Поэтому условия функционирования ведомственных систем управления и связи и системы воздействия взаимосвязаны. Это даёт возможность на основании выбора стратегии системы воздействия обосновать направления защиты системы связи (СС) в условиях информационного противоборства. С этой целью, на основании анализа системы воздействия противника, её структуры, основных функций, принципов действия необходимо прогнозировать распределение средств воздействия по элементам СС с учётом места и роли объектов в системе, очерёдность поражения объектов СС и выявлять наиболее опасные виды воздействия (синтез стратегии системы воздействия). В дальнейшем это позволит формировать исходные данные для реализации синтеза оптимальной (с точки зрения защищённости) структуры СС для заданных условий.

Одной из форм воздействия на СС является радиоподавление (РП) радиоэлектронных средств СС. Одним из требований к РП сегодня является противодействие не отдельным средствам, а в целом системе связи с целью дезорганизации системы управления войсками и оружием.

Используемый ранее подход к обеспечению помехозащищенности сетей связи основан на разработке комплекса мер защиты точечных объектов. Анализ этих подходов показал отсутствие макроструктурных способов решения проблемы обеспечения помехозащиты сетей связи, которые учитывали бы их структурно-топологические характеристики. Такой подход не позволяет дифференцированно подходить к противодействию РП.

Проведенный анализ системы РП позволяет сделать вывод, что различные технические средства РП (ТСРП) вносят неравнозначный вклад в подавление СС. Так как СС - сложная система, обладающая взаимосвязями, то необходимо решить задачу по определению оптимальной стратегии противника, где учитывались бы не только энергетические, временные и частотные характеристики объектов связи. С учетом различной эффективности средств РП, функциональной взаимосвязи и важности элементов СС необходимо решить задачу синтеза оптимальной стратегии РП.

Целью методики является прогнозирование распределения средств РП противника с учётом места и роли линий связи в защищаемой системе, определение очерёдности подавления линий связи и наиболее опасных средств РП, что, в свою очередь, позволит формировать исходные данные для принятия мер по защите СС.

Таким образом, синтез стратегии РП сводится к решению задачи распределения разноэффективных ТСРП по взаимозависимым, с различной степенью важности элементам так, чтобы вероятность их подавления (математическое ожидание числа подавленных элементов) была максимальна с учетом их веса в сети (задача распределения ограниченного неоднородного ресурса по взаимозависимым элементам сети)

Методом решения задачи является метод двух функций (модернизация градиентного метода с учетом последовательной процедуры динамического программирования).

Бунин А.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ЭТАПЫ РАЗРАБОТКИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙВЫЧИСЛИТЕЛЬНОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящее время одной из наиболее популярных технологий для организации беспроводного доступа является технология Wi-Fi (Wireless Fidelity, в переводе - беспроводная точность). Соответственно, локальные сети имеют аббревиатуру WLAN (Wireless LAN). Сеть WLAN – это беспроводная локальная вычислительная сеть (БЛВС), использующая для передачи данных высокочастотные радиоволны. Такая сеть может использоваться как альтернатива или как расширение для проводных вычислительных сетей.

Беспроводные сети основаны на стандарте IEEE 802.11 и могут работать в нескольких режимах, а их реализация отличается в зависимости от стандарта. Из всех существующих стандартов IEEE 802.11 на практике чаще всего используются следующие стандарты: 802.11a, 802.11b, 802.11g, 802.11i, 802.11n. Они различаются по частотному диапазону, методу и скорости передачи данных, дальности связи и другим характеристикам.

Более новая технология WiMAX основана на стандарте IEEE 802.16, позволяет предоставлять услуги беспроводного широкополосного доступа. Продукты WiMAX представляют собой модели как для фиксированного, так и для мобильного доступа с портативных устройств. Стандарт IEEE 802.16 разработан для работы в условиях частичного или полного отсутствия прямой видимости с базовой станцией при радиусе покрытия сектора от 3 до 10 километров.

В общем случае методика разработки (проектирования) БЛВС специального назначения, как определённая последовательность применяемых стандартов, методов и средств для достижения поставленной цели, включает в себя ряд этапов, заканчивающихся заданным результатом:

– формирование требований к БЛВС;
– разработка концепции БЛВС;
– разработка и утверждение технического задания на создание БЛВС;
– разработка предварительных и окончательных проектных решений по БЛВС и её частям, а также документации на них.
– Исходными данными для выполнения проектирования беспроводных ЛВС могут выступать:
– требования руководящих документов по разработке комплексов и средств автоматизации и связи;
– теоретические положения и материалы по технологиям БЛВС;
– тактико-технические характеристики средств автоматизации;
– материалы по возможностям применения беспроводных ЛВС специального назначения.

К основным требованиям при разработке БЛВС, как сложных автоматизированных систем, относят нормативные и технические требования: по производительности (пропускной способности), по надежности и безопасности, по расширяемости и масштабируемости, по управляемости, по совместимости программного обеспечения и некоторые другие.

На начальных этапах проектирования предлагается использовать методы математического моделирования, среди которых широко используется имитационное моделирование. При этом в качестве инструментальных средств разработчика моделей хорошо зарекомендовали себя такие средства как GPSS-PC, GPSS World, AnyLogic.

Бунин А.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИМИТАЦИОННАЯ МОДЕЛЬ ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙВЫЧИСЛИТЕЛЬНОЙ СЕТИС БАЗОЙ ДАННЫХ

При проектировании и исследовании средств и комплексов автоматизации управления широко применяется имитационное моделирование с применением ЭВМ. Для повышения эффективности процесса моделирования применяются специализированные средства и языки имитационного моделирования, ориентированные на конкретные объекты исследования. При моделировании автоматизированных информационных систем для расчёта значений вероятностно-временных показателей своевременности и надёжности эти системы сводятся к системам и сетям массового обслуживания (СМО, СеМО). Наиболее приспособленным языком описания СМО является язык GPSS, который принят в качестве базового.

Большинство элементов автоматизированных систем имеет сложную структуру и характеризуется многообразием связей между элементами. Примерами являются персональные ЭВМ, локальные вычислительные сети (ЛВС) и др.

Возвращаясь к примеру с ЭВМ и ЛВС, можно сказать, что пользователи сети выступают в роли источника потока запросов на решение задач (заявок). Заявки, поступающие в случайные моменты времени, образуют входной поток заявок. ЭВМ сети, беспроводный канал передачи данных интерпретируются обслуживающими приборами. Заявки, которые не могут быть приняты к обслуживанию, образуют очередь. Результаты решения задач формируются в выходной поток заявок.

Результатом исследования, как правило, выступают временные характеристики процесса пребывания заявки в отдельных СМО сети. Это время ($t_{пр}$) определяется двумя составляющими: временем ожидания обслуживания ($t_{ож}$) и временем собственно обслуживания ($t_{обс}$): $t_{пр} = t_{ож} + t_{обс}$. Оба слагаемых являются случайными величинами. Следовательно, время пребывания заявки в СеМО также случайно. Поэтому уместно вести речь об определении числовых характеристик этой величины, например, среднего значения $M[t_{пр}]$ или дисперсии $D[t_{пр}]$, а возможно и функции распределения $F(t_{пр})$ или функции плотности $f(t_{пр})$.

В разрабатываемой модели с каждойЭВМ пользователи могут формировать два типа запросов к базе данных (БД), ведущейся в центральной ЭВМ:запросы на выдачу данных из БД (тип 1);запросы на корректировку данных в БД (тип 2).

Названные типы запросов отличаются маршрутами их выполнения.

Запросы типа 1 формируются на ЭВМ пользователей, передаются по каналам передачи данных, обрабатываются в центральной ЭВМ и результаты поступают по каналам передачи данных на пользовательские ЭВМ, где преобразуются в форму, удобную для пользователей.

Запросы типа 2 также формируются на ЭВМ, передаются по каналам передачи данных и обрабатываются в ЭВМ с БД. На этом их исполнение завершается.

Процесс имитации прохождения заявок такой СеМО, можно представить последовательностью действий, называемой моделирующим алгоритмом.Схема СеМО, интерпретирующей рассмотреннуюЛВС, представлена определённой структурой СМО.

Вартанова Е.Ю.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Информация в современном мире - это самая ценная вещь, за которую идет постоянная борьба. Каждый человек сталкивался с кражей, незаконным распространением той или иной информации, наносящей вред личности, обществу, государству. Информационная безопасность телекоммуникационных систем нередко сводится к компьютерной безопасности. Она так же подвержена множеству угроз. Основными видами этих угроз являются:

- Нормативно-правовые;
- Физические поломки;
- Аппаратно-программные;
- Радиоэлектронные помехи;
- Информационные.

Радиоэлектронные помехи связаны в своем роде с «закладками». Информационная безопасность может оказаться под угрозой из-за звукозаписывающей «закладки», которую злоумышленник может вставить в телефон и с помощью нее узнать конфиденциальную информацию.

К физическим помехам относится, непосредственно, поломка, уничтожение, похищение информационных носителей.

Аппаратно-программные угрозы связаны с вирусами, которые могут не только замедлить скорость передачи данных и прервать ее, но и способствуют краже информации.Информационные угрозы связаны с нарушением при сборе информации, ее обработке и передачи.

Для защиты информации в телекоммуникационных системах используют:

- «Заглушки»;
- Антивирусные программы;
- Аутентификацию пользователя и др.

Так же, для защиты он несанкционированного доступа к информации, необходим обученный персонал, который владеет определенными навыками для защиты информации.

ВасюковД.Ю.,. ЛаутаО.С, Ефаров,И.А., ЛаутаА.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНЫХ АТАК

Компьютерная атака – несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Результатом воздействия компьютерных атак являются блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в автоматизированных системах управления, отказы, сбои в работе информационно-телекоммуникационной сети (ИТКС), а также компрометация передаваемой (получаемой) информации.

Компьютерные атаки обладают вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень их опасности, выбрать и реализовать меры защиты. Для исследования и определения ВВХ компьютерных атак необходима разработка их моделей.

С этой целью предлагается использовать профильные модели атак и метод топологического преобразования стохастических сетей (ТПСС).

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 компьютерных атак позволит обосновать направления разработки системы защиты ИТКС, целью которой является предотвращение (затруднение) реализации компьютерной атаки.

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

СИСТЕМНЫЕ ИССЛЕДОВАНИЯ ВЫБОРА И ОБОСНОВАНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА И КРИТЕРИЕВ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Оснащение ВС РФ современными видами вооружения и военной техники, направленной на повышение эффективности применения войск при ведении боевых действий, при решении задач в конфликтах, при выполнении сложных и опасных задач с минимальными потерями личного состава, является приоритетной задачей. С этой целью разрабатываются системы и комплексы вооружения, включая комплексы с беспилотными летательными аппаратами (КБЛА).

Состав, структура и задачи КБЛА позволяют их охарактеризовать как сложные динамические системы, что предусматривает применение методов системного анализа для их совершенствования и эффективного применения.

Основными путями совершенствования КБЛА являются:

– применение новых методов обработки командно-программной и целевой информации;

– оптимизация структуры системы управления и использование новых способов и алгоритмов управления БЛА;

– перераспределение функций и задач в КБЛА.

Общей целью совершенствования КБЛА является повышение эффективности использования возможностей объекта управления (БЛА), которое обеспечивает следующие направления:

1. Повышение оперативности управления.

2. Снижение затрат ресурсов на выполнение информационных и расчетных задач.

3. Повышение степени научной обоснованности принимаемых решений на основе анализа и прогноза событий информационного противоборства.

Поскольку информация, используемая в КБЛА для достижения целей надсистемы, может быть как пригодной, так и в результате воздействия деструктивных факторов стать непригодной для этого, к ней предъявляются определенные требования в соответствии с ее назначением.

Качество информации – совокупность свойств информации, обусловливающих ее пригодность удовлетворять определенные потребности в соответствии с назначением. Как любая система специального назначения, КБЛА потенциально подвержены угрозам, в том числе, направленным на нанесение ущерба ее информационным ресурсам, то к качеству информационно-программного обеспечения (ИПО) предъявляются требования, которые целесообразно описать показателями, характеризующими, с одной стороны, ценность информации для надсистемы в соответствии с целевой функцией КБЛА, а с другой – безопасность, как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Таким образом, от правильного выбора вектора показателей качества (ИПО) зависит эффективность функционирования КБЛА. Научно обоснованный выбор показателей качества ИПО позволит достигнуть оптимальных (рациональных) решений путем перераспределения ограниченных ресурсов КБЛА.

Воронков К.Л., Труфанов С.К.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ ДАННЫХ МОНИТОРИНГА СОБЫТИЙ БЕЗОПАСНОСТИ

В современных системах управления событиями информационной безопасности (SIEM) постоянно формируется и хранится огромное количество событий, связанных с функционированием информационной системы.

Для эффективного анализа поступающих данных необходима организация хранилища данных, обеспечивающего возможность выполнения тех или иных аналитических функций. В качестве методов, используемых при ретроспективном анализе данных, могут использоваться методы, относящиеся как к методам статистической обработки, так и к методам интеллектуального анализа данных, (т. н. Data Mining).

Среди методов статистической обработки могут использоваться следующие:

– корреляционный анализ;
– регрессионный анализ;
– канонический анализ;
– кластерный анализ;
– факторный анализ;
– анализ главных компонент и др.

Использование статистических методов требует наличие априорного представления о закономерностях, которые смогут быть выявлены путем анализа.

В связи с тем, что множество возможных деструктивных воздействий на защищаемые элементы информационной и телекоммуникационной системы непрерывно расширяется — возникают новые и модифицируются уже известные угрозы, целесообразно проводить анализ, позволяющий обнаруживать ранее не известные закономерности. Действия по выявлению таковых возможны с использованием методов Data Mining, например:

– использование деревьев решений;

– применение искусственных нейронных сетей.

Перманентное хранение данных о событиях, происходивших в системе связи, позволяет использовать их для ретроспективного анализа, направленного на выявление скрытых закономерностей. Выявление этих закономерностей позволяет обнаруживать потенциальные угрозы информационной безопасности, а также формировать рекомендации по их устранению. Оценивать эффективность принятых мер по устранению выявленных угроз можно также с помощью ретроспективного анализа.

Воронков К.Л., Таран В.В. Шерстюк Ю.М.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СРЕДСТВ УПРАВЛЕНИЯ С ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ

С позиций контроля и управления телекоммуникационным оборудованием (ТКО), выступающим в качестве объектов мониторинга и управления в автоматизированных системах управления связью (АСУС) в контексте информационной безопасности существенны множество разноплановых классификационных признаков ТКО – таких как:

1) наличие сертификата соответствия предъявляемым требованиям по информационной безопасности;

2) категория производителя оборудования – отечественный (имеющий статус доверенного производителя или не имеющий такового) или зарубежный;

3) тип программного обеспечения, используемого в ТКО (внесистемное, системное);

4) поддерживаемые ТКО протоколы взаимодействия с внешними по отношению к нему средств мониторинга и управления;

5) возможность управления ТКО с использованием протоколов мониторинга и управления;

6) наличие встроенных в ТКО средств разграничения доступа, антивирусных средств, средств контроля версий и целостности программного обеспечения, конфигурационных файлов;

7) возможность шифрования трафика мониторинга и управления;

8) наличие выделенного порта для мониторинга и управления (физического или логического);

9) возможность образования технологического тракта, обеспечивающего передачу трафика мониторинга и управления по отношению к удаленному однотипному оборудованию;

10) ведение ТКО внутренних журналов регистрации событий;

11) наличие систем (средств) управления, предоставляемых производителем, и их возможности по контролю параметров информационной безопасности ТКО

и других.

Для унификации информационных взаимодействий средств управления АСУС с ТКО предлагается использовать морфологическую модель, отражающую основное содержание и варианты взаимодействий. В основе модели лежит использование параметрической информационной базы управления ТКО (Management Information Base (MIB)), доступной по событийному и параметрическому интерфейсам и протоколам, обеспечивающим использование этих интерфейсов.

Также в общем случае ТКО может поддерживать интерфейс командной строки (Command Line Interface (CLI)) и/или файловый интерфейс (интерфейс манипулирования файлами).

Существенно, что для того или оного оборудования:

– выполнение определенных действий, связанных с запуском и выполнением вычислительных процессов в ТКО, может быть выполнено посредством команд CLI или путем изменения значений параметров MIB;

– параметры MIB могут быть доступны на чтение, на чтение-запись или только на запись;

– конфигурационные параметры ТКО и регистрационные журналы могут быть представлены только параметрами MIB, только файлами или тем и другим, причем в последнем случае взаимно-однозначного соответствия может и не быть (например, в файловых журналах хранится больше сведений, чем в их представлении в MIB);

– файлы могут быть в той или иной мере представлены в MIB (например, имена и размер файлов конфигурации, контрольная сумма файлов программного обеспечения и т.д.).

Таким образом, возможные сочетания информационного взаимодействия средств управления с ТКО определяются его технической реализацией и подлежат учету при создании программных средств АСУС.

Разработанная морфологическая модель описывает возможное сочетание:

– видов мониторинга ТКО – оперативный и ретроспективный, параметрический и событийный;

– способов взаимодействия с ТКО – непосредственное или опосредованное (через разного рода шлюзы информационных взаимодействий, системы управления производителей и т.д.);

– способов получения данных мониторинга – чтение содержимого файлов ТКО, использование службы syslog, SNMP-агентов ТКО и т.д.

Предложенная модель может служить методической основой для реализации унифицированных средств мониторинга и управления ТКО в виде инвариантного программного ядра и модулей адаптации, состав которых может изменяться в процессе эксплуатации АСУС – как следствие динамики парка контролируемого и управляемого ТКО.

Вотинов М.Л., Ковайкин Ю.В., Пичугин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРИЧИНЫ ВОЗМОЖНОЙ УТЕЧКИ ОПТИЧЕСКОГОИЗЛУЧЕНИЯ ИЗ ОВ ВОЛС

Одно из принципиальных преимуществ волоконно-оптических линий связи (ВОЛС) по сравнению с другими – повышенная скрытность передаваемых оптических сигналов. Конструкция оптических кабелей такова, что излучение через боковую поверхность оптического волокна (ОВ) эффективно экранируется защитными оболочками и элементами конструкции кабеля. Только наружная оболочка кабеля обеспечивает экранировку в *80÷120* дБ, что снижает уровень мощности ниже квантового предела обнаружения. Технологический и эксплуатационный контроль позволяет поддерживать указанные параметры в течение всего срока эксплуатации волоконно-оптической линии. Поэтому, оптические кабели в отличие от радиочастотных не нуждаются в контролируемой зоне. Тем не менее, применение ВОЛС полностью не обеспечивает защищенность передаваемой информации. Небольшая часть оптического излучения, в результате специальных действий противника, все же может быть выведена из ОВ, а при наличии высокочувствительной оптико-электронной аппаратуры, может быть сфокусирована и продетектирована.

В основе утечки оптического излучения лежит какое-либо физическое явление, которое за счет воздействий на ОВ, приводит к увеличению рассеиваемой мощности, т.е. к изменению характеристик направленного излучения в ОВ.

Причиной изменения характеристик распространения направленного излучения является неоднородность характеристик ОВ. Неоднородности в основном приводят к двум физических явлениям в ОВ: рассеянию оптического излучения и взаимодействию мод. Рассеяние в основном определяется нарушением геометрической формы ОВ. Рассеяние сильно возрастает при наличие последовательности очень малых изгибов.

Взаимодействие мод проявляется в обмене энергией между ними. Обмен энергией существенно увеличивается, когда картины полей мод перекрываются в значительной степени. Неоднородности наиболее эффективно содействуют этому обмену, если расстояние между ними равно периоду биений между двумя взаимодействующими модами.

В основе превращения направленного излучения в ненаправленное лежат два основных эффекта в ОВ, получившие название "модовая оптика" и "преобразование мод". Причины возникновения неканализируемого излучения, как частного случая ненаправленного, которое затем легко вывести за пределы ОВ.

Причины возникновения неканализируемого излучения:

– Преобразование мод высоких порядков, близких к частоте отсечки ОВ, в моды излучения в оболочке;

– Образование оболочечных (мод излучения в оболочке) и вытекающих из сердцевины ОВ мод (быстрозатухающих и слабозатухающих) при вводе в ОВ полного спектра мод от диффузного источника излучения или от источника, чья пространственная диаграмма излучения превышает числовую апертуру ОВ;

– Возбуждение затухающих мод при плохом согласовании отрезков ОВ (при разъемном и сварном соединении);

– Образование вытекающих мод из сердцевины ОВ за счет рэлеевского рассеивания;

– Рэлеевское рассеяние мод, распространяющихся в оболочке;

– Перенос энергии от световодных мод высокого порядка к вытекающим модам в результате взаимодействия между модами разных групп;

– Рассеяние светового излучения на микрофлуктуациях плотности вещества (бриллюэновское рассеяние), вызванных гиперзвуковыми колебаниями молекул;

– Причины определяют возможность перехвата информационного излучения, распространяющегося в ОВ. Вспомогательные воздействия нарушителя на ОВ, приводящие к образованию неканализируемого излучения, будем называть способами перехвата информации, передаваемой по ВОЛС.

Вотинов М.Л., Ковайкин Ю.В., Титова И.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРИМЕНЕНИЕ КВАНТОВОЙ КРИПТОГРАФИИ В ТКС

Идея использовать квантовые объекты для защиты информации от подделки и несанкционированного доступа впервые была высказана учеными еще в 1970 годах, которые были знакомы с работой Вейснера, они предложили использовать квантовые объекты для передачи секретного ключа. В 1984 г. они опубликовали статью, в которой описывался протокол квантового распространения ключа ВВ84.

Носителями информации в протоколе ВВ84 являются фотоны, поляризованные под углами 0, 45, 90, 135 градусов.

В основе метода квантовой криптографии лежит в наблюдении квантовых состояний фотонов. Отправитель задает эти состояния, а получатель их регистрирует. Здесь используется квантовый принцип неопределенности Гейзенберга, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Таким образом, если отправитель и получатель не договорились между собой, какой вид поляризации квантов брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации. Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа.

Ученые из Бристольского университета предложили для регистрации изменений в переданных с помощью квантовых преобразований данных использовать следующийалгоритм:

Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.

Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).

Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.

Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.

Чтобы исключить кратные ошибки, которые могут быть не замечены, операции предыдущих пунктов повторяются для большего значения k.

Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки, а именно: получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках; получатель и отправитель открыто сравнивают четности (если строки отличаются, четности должны не совпадать с вероятностью 1/2); если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.

Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2-m.

Квантовая криптография − чрезвычайно надежный в теории метод защиты каналов связи от прослушивания, однако на практике реализовать его пока довольно трудно. На обоих концах канала должна быть установлена сложная аппаратура − источники одиночных фотонов, средства управления поляризацией фотонов и чувствительные детекторы. При этом для измерения угла поляризации фотонов необходимо точно знать, как ориентировано оборудование на обоих концах канала.

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

ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности в автоматизированную систему специального назначения (АССН).

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:целостность данных, конфиденциальность информации и доступность информации для всех авторизованных пользователей.

Известно много мер, направленных на обеспечение информационной безопасности, одними из которых являются организационные.

Организационная защита информации - составная часть системы защиты информации АССН, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечениязащиты информации.

Основными направлениями организационнойзащиты являются: организация работы с персоналом, организация пропускного режима и охраны, организация работы с носителями сведений составляющих государственную тайну, комплексное планирование мероприятий по защите информации, организация аналитической работы и контроля.

Методы защиты информации в АССН направлены на решение следующих задач:реализация эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение ее утечки, осуществление принципа персональной ответственности командиров (начальников) подразделений и должностных лиц за защиту конфиденциальной информации, определение перечней сведений, относимых к различным категориям (видам) конфиденциальной информации, ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени ее конфиденциальности, подбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение должностных лиц, допущенных к конфиденциальной информации, организация и ведение конфиденциального делопроизводства, осуществление систематического контроля за соблюдением установленных требований по защите информации.

Гусенцова П.Г., Закалкин П.В., Кузнецов С.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕШЕНИЯ ЗАДАЧИ КОНТРОЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

В последнее время одним из наиболее перспективных и развивающихся направлений построения сетей связи в мире являются волоконно-оптические линии связи (ВОЛС). Это объясняется тем, что они значительно превосходят радио-радиорелейные и проводные линии по таким свойствам (характеристикам) как: пропускная способность, помехозащищенность, протяженность регенерационного участка.

ВОЛС состоят из стационарного оборудования, размещаемого на точечных объектах, и линейного тракта, представляющего собой волоконно-оптические кабели и усилители оптического сигнала.

Защита стационарного оборудования обеспечивается точно так же как и защита любого аналогичного объекта и имеет мало особенностей, в то время как защитить линейную часть на всем её протяжении достаточно сложно как в техническом, так и в финансовом плане.

Ситуацию усугубляет то, что до недавнего времени считалось, что волоконно-оптические линии связи обладают высокой защищенностью от несанкционированного доступа.

Поскольку волоконно-оптический кабель практически не излучает в радиодиапазоне, то передаваемую по нему информацию трудно перехватить не нарушая процесса приема-передачи. Однако последние исследования доказывают уязвимость ВОЛС.

Таким образом, на первый план выходят задачи контроля информационной безопасности (ИБ) ВОЛС (а в частности контроля несанкционированного доступа к ВОЛС).

Контроль состояния и измерение параметров ВОЛС необходимо проводить как во время монтажа, так и в процессе эксплуатации.

В настоящее время при измерении параметров оптического тракта наиболее распространенным является рефлектометрический метод, в основе которого лежит использование оптических рефлектометров (OTDR, Optical Time Domain Reflectometer). Однако требования к их тактико-техническим характеристикам в целях контроля ИБ ВОЛС не определены.

Предлагается ввести следующую классификацию основных характеристик современных оптических рефлектометров:

- динамический диапазон;
- мёртвые зоны (затухание и событие);
- рабочая длинна волны;
- разрешение;
- возможность установки пороговых значений «Pass/Fail» («годен/не годен»);
- тип оптического интерфейса;
- интерфейсы для подключения дополнительного оборудования необходимого для диагностики ОК или оптических разъемов;
- последующая обработка полученных данных и создание отчётов.

Введение новой более подробной классификации позволит

осуществлять более точный и быстрый выбор рефлектометра необходимого для использования на конкретной ВОЛС.

производить измерения в заданном диапазоне и с заданной точностью.

зная основные характеристики существующей ВОЛС заранее составить технический парк оборудования необходимого для диагностики линии.

Таким образом, первоочередными задачами в области контроля ИБ ВОЛС требующими решения являются:

1. Обоснование тактико-технических характеристик средств контроля ИБ ВОЛС;
2. Обоснование точек установки средств контроля на цифровых сетях связи, созданных на базе ВОЛС.

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

МОДЕЛЬ ПРОЦЕССА КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

В связи с большим количеством объектов информатизации поток заявок на проведение аттестаций и спецобследований инструментальным методом значительно увеличивается. Однако в настоящее время существующие органы контроля из-за ограниченности ресурса не в состоянии в полной мере справиться с возложенной на них задачей.

Обеспечение своевременности, полноты, непрерывности и достоверности контроля станет возможным только при условии организации не только плановых проверок, но и оперативного "сопровождающего" контроля защищенности информации на всех объектах информатизации.

Под "сопровождающим" контролем защищенности информации на объектах информатизации предлагается понимать оперативную проверку объектов информатизации и мест деятельности должностных лиц органов управления на предмет отсутствия технических каналов утечки информации непосредственно перед началом обработки и в течение всего периода обработки.

Обеспечение указанного типа контроля возможно только при наличии специального подразделения, оснащенного мобильным комплексом технических средств контроля.

Ввиду достаточно широкого спектра уже разработанных технических средств выявления каналов утечки информатизации для такого комплекса необходимо определить целесообразную его структуру, состав и возможности реализации заданных характеристик на базе известных технических решений.

Исходными данными для МПКЗИ является количество проведенных проверок, количество бригад и личного состава в них.

В целях исследования своевременности процесса контроля в рамках методики были разработаны модели для определения количества бригад, осуществляющих контроль защищенности информации от утечки по техническим каналам и личного состава в них.

Они представляют собой многоканальные СМО, без отказов с очередью, с экспоненциальными законами распределения времени поступления и обслуживания заявок.

Правильное распределение сил и средств контроля невозможно без предварительной оценки затрат времени, требуемых для выполнения каждой из запланированных работ.

Средние затраты времени на отдельные операции были определены методом экспертных оценок специалистами контроля с учетом накопленного опыта работ в ходе аналогичных проверок, объёма и других характеристик объектов (помещений), намеченных для проведения проверки.

Результаты, полученные в ходе решения, дают основание утверждать, что разработанная математическая модель отражает реальный процесс КЗИ от ее утечки по техническим каналам.

Степень адекватности МПКЗИ в работе оценивается по основным группам показателей, соответствующим основным этапам разработки математической модели:

– полноте отображения и точности взаимосвязей основных процессов (экстенсивные показатели);
– глубине и существенности отображения основных факторов (интенсивные показатели);
– достоверности (доказательности) отображения.

При оценке адекватности аналитической МПКЗИ на объектах информатизации, получены количественные значения параметров разработанной модели, позволяющие сделать вывод о точности и полноте учета в ней физических свойств реального процесса, что в свою очередь, позволяет говорить об адекватности аналитической МПКЗИ на объектах информатизации реальному процессу.

Разработанная МПКЗИ позволяет обоснованно подойти к выбору количества личного состава в бригаде и количества бригад, что существенно повышает эффективность мероприятий контроля защищенности информации на объектах.

На основе МПКЗИ разработана методика оценки своевременности контроля защищенности информации на объектах информатизации, которая позволяет оценивать своевременность контроля по показателям вероятности и среднему времени контроля защищенности информации.

На ее основе разработаны предложения по составу сил органов контроля защищенности информации.

Дементьев В.Е., Коцыняк М.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПОДХОД К ОЦЕНКЕ ПРОТОКОЛЬНОЙ ЗАЩИЩЕННОСТИ ИТКС

Проблема обеспечения информационной безопасности (ИБ) стоит в ряду первостепенных задач при проектировании информационно-телекоммуникационных сетей (ИТКС).

Поскольку ИТКС является результатом конвергенции компьютерных и телекоммуникационных сетей, ее функционирование осуществляется в условиях воздействия некоторой совокупности информационных угроз, направленных на ее элементы и негативно влияющих тем самым на ее эффективность.

В связи с этим важной задачей является обеспечение достаточной степени защищенности ИТКС в этих условиях, для чего в свою очередь необходимо наличие адекватного аппарата, позволяющего оценить возможные методы и способы воздействия и проявления угроз на ИТКС.

В ряду наиболее актуальных угроз, существенно влияющих на общий уровень защищенности ИТКС, стоят различные информационные воздействия (ИВ).

По своей сути эти воздействия сводятся к эксплуатации общеизвестных принципов и способов обработки данных, т.е. протокольного взаимодействия между различными элементами сети. В общем виде протокол – это совокупность правил и процедур, определяющих взаимодействие и обмен данными между устройствами, абонентами и уровнями ИТКС.

Тогда протокольное воздействие – заранее спланированное целенаправленное воздействие на протоколы информационного обмена, обмена данными, функционального и другого назначения через установление или нарушение соединения или попытки установления или нарушения соединения на уровнях эталонной модели взаимодействия открытых систем или других известных моделях Интернета с объектом данного воздействия.

Цель протокольного воздействия – организация канала утечки информации, модификация, уничтожение информационных ресурсов, блокирование (перевод во внештатный режим работы) системы защиты информации, а так же изменение штатного функционирования ИТКС, приводящее к нарушению или блокированию информационного обмена.

Таким образом, в случае, когда речь идет о протокольной защищенности, мы говорим не о состоянии ИТКС, которое влияет на уровень ее защиты (или защиты информации, в ней обрабатываемой), а о некоторой совокупности признаков, наличие которых позволяет говорить о возможных ИВ на ИТКС. Наличие или отсутствие подобных ИВ определяется совокупностью информационных признаков, характерных для того или иного протокола ИТКС. Каждый из признаков обладает определенным уровнем информативности, по которому определяется степень опасности протокола для ИТКС.

Таким образом, на первом этапе определяется совокупность критически важных информационных признаков и их степень информативности.

Кроме того, немаловажное значение имеет уровень ИТКС (в соответствии с моделью ЭМВОС) и набор протоколов соответствующего уровня.

Для определения априорной и апостериорной иерархичности ИВ в рамках методологического подхода необходима оценка важности уровней и протоколов ИТКС, что в дальнейшем позволит получить исходные данные для прогнозирования вероятностей воздействия на протоколы ИТКС.

В итоге полученные исходные данные могут быть использованы для оценки протокольной защищенности ИТКС путем определения коэффициентов надежности и стойкости каждого протокола, участвующего в информационном обмене ИТКС и формирования матриц защищенности, позволяющих спрогнозировать общий уровень защищенности ИТКС от протокольных воздействий.

Таким образом, для оценки протокольной защищенности ИТКС ВН необходимо определить вероятности информационных воздействий на ИТКС.

Для этого необходимо разработать подход, который бы включал оценку информативности признаков протоколов ИТКС ВН, оценку комплексного информационного воздействия на протоколы ИТКС ВН, а так же оценку протокольной защищенности ИТКС ВН.

Полученные в результате расчетов значения могут быть использованы в дальнейшем в качестве исходных данных для синтеза системы протокольной защиты ИТКС ВН.

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

МОДЕЛИРОВАНИЕ СУБД КАК СИСТЕМЫ СМАССОВЫМ ОБСЛУЖИВАНИЕМ

Автоматизированную информационную системуспециального назначения(АИС СН), построенную по концепции баз данных (БД), в процессе моделирования необходимо рассматривать как систему с массовым обслуживанием (СМО). Это обусловлено следующими факторами:

1. Имеется поток запросов на обслуживание к БД, который носит случайный характер.

2. Наличие очереди запросов.

3. Обслуживание запросов программными средствами СУБД осуществляется в течении некоторого промежутка времени, который также носит вероятностный характер.

Следовательно, СУБД, как элемент АИС СН, целесообразно представлять как СМО.

В зависимости от цели исследования это может быть одноканальная СМО, многоканальная СМО, а также сеть с массовым обслуживанием.

Оценку качества ИП в СУБД целесообразно проводить по количественным показателям.

При оценке оперативности получения информации из баз данных, таким показателем будет математическое ожидание случайной величины, например, среднее время, определяемое двумя составляющими: средним временем ожидания обслуживания и средним временем обслуживания.

МоделироватьСУБД как СМО необходимоимитационными методами, так как они позволяют учесть особенности структуры базы данных.

Информационные процессы в приборах обслуживания будут носить вероятностный характер и для обобщенной модели вероятность случайной величиныбудет иметь нормальное распределение, что доказывают проведенные исследования.

Учитывая, что пользователи могут формировать запросы двух типов: запрос на поиск информации в базе данных и запрос на корректирование информации в базах данных, возможно построения более точной модели.

В случае запроса на поиск, время обслуживания будет равно времени поиска информации СУБД, а при корректировке информации учитываетсякак время на поиск, так и время на корректировку информации СУБД.

При дальнейшем уточнении модели прибор обслуживания можно декомпозировать на составляющие.

Таким образом, реализация имитационной модели позволит осуществить оценку качества информационных процессов в системах управления базами данных АИС.

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

ВЫБОРПОКАЗАТЕЛЕЙ КАЧЕСТВА СУБД ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

К управлению в системах военного назначения применяются следующие требования – устойчивость, непрерывность, оперативность и скрытость. Исходя из этого можно сделать вывод, к свойствам систем управления военного назначения можно отнести степень выполнения системой данных требований. Будет справедливым сказать, что к составные части систем управления будут так же обладать аналогичными свойствами.

Одним из основных составляющих автоматизированных систем управления, оказывающих влияния на степень выполнения требований к управлению, являются автоматизированные информационные системы (АИС), основой которых, в свою очередь, являются базы данных.При проектировании АИС для достижения высокого качества большую роль будет играть выбор СУБД.

Оценку СУБД можно провести по совокупности свойств. Исходя из выше изложенного, в АИС СпН в качестве основных свойств, определяющих назначение информационных процессов, целесообразно использовать оперативность, скрытность, устойчивость и достоверность. Устойчивость в свою очередь является сложным свойством, которое характеризуется живучестью, помехоустойчивостью и др.

Каждый запрос к базе данных требует его обработки в течение некоторого случайного промежутка времени, зависящего от содержания запроса, длинны очереди запросов. Таким образом, работу АИС можно рассматривать как операцию массового обслуживания, состоящую из элементарных операций – ожидания в очереди и обработки отдельных запросов. Исходя из этого количественные показатели оценки качества информационные процессы в базах данных (ИП) будут вероятностными. Так оперативность можно оценивать по среднему времени ответа на запрос к БД, скрытность – по вероятности несанкционированного доступа к БД, достоверности – вероятности искажения информации в БД за время *T*.

Обобщенные показатели качества ИП на предпроектной стадии декомпозируются на частные показатели. На примере оперативности частными показателями будут: среднее временя корректировки информации в БД и среднее временя поиска информации в БД.

Проведя оценку СУБД по частным показателям качества и выбрав из всего множества СУБД, удовлетворяющие требованиям, на стадии технического проекта частные показатели качества также декомпозируются, после чего проводится оценка оставшихся СУБД.

В результате проведения оценки качества выбирается СУБД максимально удовлетворяющая требованиям.

Долгая А.А., Шункова И.Ю., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ДАННЫХ

Задача надежной защиты информации от несанкционированного доступа является одной из основных и не решенных до настоящего времени проблем. Одним из направлений ее решения является применение средств и методов компьютерной стеганографии.

Компьютерная стеганография – это сокрытие сообщения или файла в другом сообщении или файле, в частности, в аудио- или видеофайле.

Возможность использования методов цифровой стеганографии объясняется особенностями функционирования зрительного и слухового аппаратов человека.

Известно, что слуховой аппарат человека функционирует в широком динамическом диапазоне. При этом он очень чувствителен к случайным аддитивным помехам, способен различать относительную фазу и совсем не чувствителен к абсолютной фазе. Эти особенности слухового аппарата позволяют удачно использовать стеганографические методы в аудиосреде.

На практике широко используются следующие методы стеганографического скрытия данных: метод наименьших значащих битов, методы широкополосного кодирования, метод сокрытия в эхо-сигнале, фазовые методы сокрытия.

Каждый из этих методов имеет свои достоинства и недостатки.

Модификация звука в частотной области потребует применения дискретного преобразования Фурье к сегментам области данных и последующей модификации значений спектра амплитуд или спектра фаз. Незначительные модификации не приведут к явному демаскированию факта стегопреобразования, но при сокрытия файлов, размер которых превышает 1/20 размера контейнера, акустические свойства звука своим очевидным искажением дадут злоумышленнику понять о том, что файл является стегоконтейнером. Причем проведение стегоанализа путем рассмотрения файла в частотной области покажет аномальные скачки составляющих спектра, что также выдаст факт искусственной модификации файла.

Метод широкополосного кодирования позволит повысить скрытность стегопреобразования, но уменьшит пропускную способность стегоканала (на 1 бит информации потребуется не менее 100 бит данных стегоконтейнера). Это приведет к снижению эффективности программного продукта и введению строгих ограничений на максимальную длину скрываемых файлов.

Метод сокрытия в эхо-сигнале сложен в своей реализации и требует повышенных требований к качеству канала связи. Стегоанализ временной области файла, модифицированного подобным образом, покажет наличие побочных эхо-сигналов, равных на амплитуде и временному сдвигу от основного сигнала, что является бесспорным доказательством искусственности его природы.

Наиболее простым считается метод замены наименее значащих бит. Его повышенная пропускная способность (1/8 объема контейнера), высокая устойчивость к стегоанализу, скрытность за счет неизменности размера контейнера после скрытия данных и слабое влияние на акустические свойства звукового файла, позволяют говорить о том, что для реализации поставленной задачи данный метод является наиболее оптимальным.

Таким образом, файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности путемзамены существующей в них информации на информацию, которую предполагается защитить. Стеганография является эффективным методом сокрытия данных и защиты их от несанкционированного или не желаемого просмотра. Применениеметодов стеганографии совместно с другими методами сокрытия данных сделало бы возможным многоуровневую защиту информации.

Егоров А.Н., Кузнецов В.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМА ВОССТАНОВЛЕНИЯ ДОСТУПА К ДАННЫМ В КОРПОРАТИВНЫХ СЕТЯХ

В условиях функционирования корпоративных сетей, в которых для передачи данных, как правило, используются защищенные каналы, предполагающие их передачу в зашифрованном виде, возникают сбои, связанные с потерей или искажением секретных ключей. В такой ситуации актуальной становится задача автоматизации восстановления этих ключей с целью обеспечения доступа к зашифрованным данным, что позволит в значительной степени снизить уровень влияния человека на восстановление работоспособности системы.

Для решения этой проблемы, в основном, применяют подходы, предполагающие резервное копирование ключей при их генерации. Копии помещаются в хранилища, из которых в случае необходимости ключ можно восстановить. Политикой безопасности определяется формат таких

копий: ключ хранится целиком в исходном или зашифрованном виде, либо он разделяется на части, которые помещаются в отдельные хранилища, и, наконец, может сохранятся ряд параметров, связанных с ключом.

Хранилища реализуются как программными, так и аппаратными средствами, которые, помимо безопасного хранения ключа, могут поддерживать функции шифрования, дешифрования, генерации ключевой пары, а также хеш-функции, что в свою очередь значительно снижает нагрузку на программную часть криптографической системы.

Достоинством такого подхода является скорость восстановления ключа. Однако, хранение копий ключей является дополнительной уязвимостью системы и требует обеспечения надёжной защиты хранилищ.

В программной оболочке распараллеливания вычислений прикладных решений (ПОР), на которую авторами получено свидетельство о государственной регистрации программы для ЭВМ № 2014619266 от 11.09.2014, был использован механизм, при котором ключ восстанавливается из исходного и зашифрованного текстов, что несомненно требует существенных временных затрат на вычисления. ПОР реализует универсальный подход к распараллеливанию прикладных решений пользователя и в настоящее время поддерживает работу с процессорами и видеокартами компании NVIDIA, используя технологию CUDA. Применение ПОР при восстановлении секретного ключа позволило поднять производительность для процессоров в 10 раз, а используя алгоритм на основе технологии CUDA скорость возрастает в 5000 раз по сравнению с последовательной реализацией.

Приведённые оценки дают существенный эффект по времени при использовании ключей, ограниченных длиной в 56 бит. Для более длинных ключей применение реализованного механизма восстановления доступа к данным становится менее эффективным.

Поднять производительность для этих ключей предлагается за счёт использования радужных таблиц – специальный вариант таблиц поиска, реализующий разумный компромисс между временем поиска по таблице и занимаемой памятью. Для их заполнения необходимо сгенерировать начальное множество ключей, по каждому из которых составляется цепочка хэшей заданной длины. Вычисляется значение хэша ключа, к которому применяется функция редукции, генерирующая следующий ключ в цепочке. Для нового ключа операции повторяются. В результате создаётся цепочка перемежающихся ключей и хешей, последовательно связанных друг с другом. В таблицу записывается только первый и последний ключ цепочки, что существенно сокращает необходимую для её хранения память. Поиск по предварительно вычисленным значениям выполняется значительно быстрее по сравнению с полным перебором, но создание самой радужной таблицы требует больших временных затрат и несмотря на эффективный метод хранения в ней данных, сгенерированные для достаточно длинных ключей таблицы могут занимают значительный объём памяти.

Для решения указанных проблем предлагается следующий подход. Дополнительно сократить время поиска ключа возможно за счёт разделения таблиц на подтаблицы так, чтобы каждая из них могла целиком обрабатываться в оперативной памяти, что повысит скорость доступа к её данным и позволит их хранить децентрализовано на различных узлах вычислительной сети. Процесс составления таблиц возможно распараллелить, что даёт возможность для повышения эффективности реализовать алгоритм на основе ПОР. Децентрализация позволяет задействовать мощность каждого из узлов сети для динамического заполнение таблиц в процессе её функционирования.

Елизаров В.В., Паращук И.Б., Салюк Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного, ОАО «ИНТЕЛТЕХ»

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ПРИМЕНЕНИЮ СРЕД И ТЕХНОЛОГИЙ РАЗРАБОТКИ ПРОГРАММНЫХ ПРОДУКТОВ В ИНТЕРЕСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В интересах информационной безопасности (ИБ), важного аспекта функционирования телекоммуникационных сетей (ТКС), всегда стараются применять самые современные среды и технологии программирования, самое развитое программное обеспечение (ПО). Одной из таких сред является среда разработки QtCreator. Это интегрированная среда разработки, которая включает инструменты для дизайна и разработки приложений.Среда Qt Creator предоставляет инструменты для решения задач разработки приложений на протяжении всего их жизненного цикла, от создания проекта до развертывания приложения на требуемой платформе. К базовым возможностям QtCreator относят: управление проектами; использование различных систем контроля версий; разработку пользовательского интерфейса; написание кода; сборку и запуск приложений; отладку и анализ, а также распространение приложений. Что касается принципов взаимодействия объектов в Qt, то для связи между объектами используются сигналы и слоты. Механизм сигналов и слотов – основная

особенность Qt, которая отличает его от других сред. Механизм сигналов и слотов возможен благодаря мета-объектной системе среды разработки QtCreator.

К новым, нетрадиционным средам и технологиям относят также так называемые технологии ко-рутинов («микронитей»). Они активно применяются для упрощения программного кода в крупных проектах, построенных на обратных вызовах (callback функциях), а также на высоконагруженных системах, активно использующих неблокирующие вызовы функций операционных систем (ОС).Принцип работы ко-рутины: при создании выделяется отдельный стек; при попадании в ко-рутину, сохраняется указатель на стек вызвавшего потока команд и его регистры; при выходе из ко-рутины сохраняется состояние регистров текущей ко-рутины и указатель на стек и восстанавливается старый контекст. Иными словами, по всем признакам ко-рутина похожа на «нить» с той разницей, что планирование не осуществляется планировщиком ОС.

К недостаткам относят: поскольку ко-рутина не «нитка», переключением контекста приходится заниматься самостоятельно; на многопроцессорной машине нельзя добиться реальной параллельности вычислений. Преимущества: в нагруженных системах, если ко-рутины обращаются к общей памяти, не происходит блокировок, поскольку ко-рутины выполняются в одной «нитке»; более читабельный код, если есть большое число однотипных действий над однотипными данными, в случае большого количества callback-вызовов; в системах с высокой нагрузкой (сервер с сотнями тысяч клиентов) хорошо экономит ресурсы ОС; быстрое (9 нс) переключение контекста между «нитями» ОС с вызовом функций ядра (этот эффект проявляется в высоконагруженных системах). Один из главных недостатков ко-рутин – невозможность добиться реальной параллельности исполнения кода, поскольку ОС планирует по CPU только «нити». Необходимость использования ко-рутин встает при обслуживании операций ввода-вывода, которые априори медленнее CPU. Тем не менее, по мере роста нагрузки, можно распределить ко-рутины по «нитям». Дескрипторов ОС (файлы, сокеты) так много в подобных системах, что проблем с распределением равномерным образом ко-рутин по «нитям» не возникает.

Таким образом, ко-рутины – тонкий программный инструмент, причем не существует универсального правила, каким образом распределять их по CPU, все зависит от внутренней архитектуры программного проекта по ИБ ТКС и требований к разработке программированию систем информационной безопасности.

Емелин В.И., Подолянец Д.В.
Россия, Санкт-Петербург, ОАО «НИИ Вектор»

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАУКОЕМКИХ ТЕХНОЛОГИЙ РАДИОЭЛЕКТРОННОГО МОНИТОРИНГА НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

В современной экономике появление инноваций непосредственно связано с созданием знаний, которые в общем случае должны содержать сведения о свойствах объектов, закономерностях процессов и явлений, а также сведения о правилах использования знаний в совокупности с уже полученными знаниями.Для создания наукоемких информационных технологий, устойчивых к деструктивным воздействиям противоборствующей стороны, строится онтологическая модель радиоэлектронной обстановки в виде непротиворечивого словаря предметной области, а также описания логики функционирования элементов обстановки, основанная на использовании парадигмы мышления, оптимальной для данной сферы деятельности.Рассматриваются инновации, которые относятся к двум наиболее взаимозависимым процессам по методологии ООН:

– инновациям, воплощенным в наукоемкие информационные технологии, охватывающие машины, технологическое оборудование, целые сооружения, производственные системы и продукцию с высокими технико-экономическими параметрами (embodiedtechnology);

– технологиям в чистом виде, охватывающими методы и технику производства товаров и услуг (dissembledtechnology).

В общем случае обеспечение безопасности наукоемких технологий предполагает выполнение комплекса мероприятий, направленных на достижение следующих целей: 1) предотвращения утечки (разглашения) информации и знаний, необходимых для успешной реализации созданного продукта на рынке продаж; 2) недопущения утраты созданной системы знаний и соответствующих им информационных ресурсов; 3) исключение преднамеренной или случайной модификации результатов интеллектуальной деятельности.

В интересах создания устойчивых информационных ресурсов и системы знаний в содержании проводимых вычислений в сфере радиоэлектронного мониторинга предлагается выделить 2 процесса.Первый из них связан с непосредственными вычислениями поступающей информации в реальном масштабе времени наблюдения за обстановкой. В структурной схеме этот процесс ограничен временем реакции системы на изменения обстановки, сложностью математического аппарата для проведения вычислений в установленный период времени и заданным перечнем входных данных наблюдения. Второй процесс вычислений предназначен для формирования гипотез, правил, допущений и ограничений, обеспечивающих получение априорной информации.

В части защиты технологий от конкурентной разведки выделены две главные проблемы. Первая проблема заключается в том, что в чистом виде не существует радиоэлектронных систем, безопасность которых в течение жизненного цикла может быть обеспечена защитой только непосредственно создаваемой системы мониторинга. На практике мы сталкиваемся с огромной гетерогенной территориально-распределенной информационной системой, в которой по мере протекания процессов жизненного цикла накапливаются определенные сведения о разрабатываемых технологиях и системе в целом. К ним относятся средства автоматизации заказчика, автоматизированные системы разработчиков и ряда других взаимодействующих систем. Таким образом, в практическом плане необходимо рассматривать вопрос защиты как минимум 2-х различных систем: 1) автоматизированная система разработки технологий радиоэлектронного мониторинга («материнская система») и 2) собственно информационная система в том виде, в котором она существует на каждом этапе (ТЗ, описания алгоритмов, технических средств, отчетов и т.д.).

Вторая проблема состоит в том, что ни одна из существующих технологий управления бизнес-процессами (например, PLM-технологий) не создавалась как информационная технология обеспечения информационной безопасности создаваемой системы мониторинга на этапе ее эксплуатации. Поэтому, как показывает практика, на этапе проектирования недостаточно уделяется внимания последствиям имевшей место утечки, утраты и модификации информации после сдачи-приемки системы. Методы оценки таких последствий вообще отсутствуют. Формирующаяся в существующих ИТ- технологиях групповая политика регламентирует доступ к документам различных пользователей после изменения состояния бизнес-процесса. Целью этих ограничений является введение запрета на изменения, просмотр или другие действия авторам и определяет права согласующим или утверждающим лицам. Формируется цепочка состояний бизнес-процесса, в которой указывается список лиц, участвующих в бизнес-процессе, а также степень их участия в согласовании и утверждении документов. Предлагается система мероприятий для использования накопленной информации в интересах обеспечения информационной безопасности на всех этапах жизненного цикла и, прежде всего, на этапе эксплуатации систем радиоэлектронного мониторинга.

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

КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕРРИТОРИЯМИ «БЕЗОПАСНАЯ ТЕРРИТОРИЯ»

Автоматизированные информационные системы (АИС), направленныена решение задач сбора, накопления, анализа информации, поддержки принятия управленческих решений в области безопасности жизнедеятельности крупных мегаполисов и промышленных территорий, особо опасных объектов и обеспечивающие повышение эффективности городского (территориального) управления, в настоящее время находят все более широкое применение. Вместе с тем их разработка и внедрение зачастую носят не системный, узковедомственный характер. При этом практически отсутствуют разработки, направленные на создание системообразующих информационных систем, обеспечивающих унифицированный доступ к функционально связанному, в рамках всех информационных систем или отдельных сфер жизни города, региона, набору услуг.

В докладе рассматриваются принципы построения системы региональной безопасности и ее основного компонента - автоматизированной информационной системы управления территориями «Безопасная территория», обеспечивающей на базе единой сетевой телекоммуникационной и вычислительной инфраструктуры эффективное объединение всех существующих региональных и ведомственных АИС в единую региональную автоматизированную информационно-техническую системуобеспечения безопасности жизнедеятельности и управления территорияей, в том числе и в период кризисных ситуаций.

Показано роль и место АИС управления территорией «Безопасная территория» в существующей инфраструктуре региональных центров управления, являющихся структурными подразделениями Национального центра управления обороной Российской Федерации и создаваемых на базе военных округов.

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

ПРОБЛЕМЫ СОЗДАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ СИТУАЦИОННЫХ ЦЕНТРОВ, КАК ЭЛЕМЕНТОВ СИСТЕМ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В последнее время в целях решения задач национальной обороны и обеспечения безопасности жизнедеятельности населения крайне актуальной стала задача создания комплексов технических средств и информационно-аналитических систем обеспечения региональной безопасности. Вместе с тем во многих регионах страны по инициативе различных министерств и ведомств (МВД, ФСБ, МЧС) уже созданы и функционируют различные системы обеспечения безопасности и противодействия ЧС.

Однако они создавались в различное время, разными ведомствами, построены по различным принципам, что усложняет их дальнейшую интеграцию в единую систему. Сейчас, в условиях создания Национального центра управления обороной страны и обострения внешнеполитической ситуации, назрела реальная потребность их интеграции в единую систему региональной безопасности, ключевым функциональным компонентом которой должен стать единый мониторинговый центр, строящийся, как правило, на базе существующего или создаваемого регионального Ситуационного центра.

В докладе рассматриваются принципы построения системы региональной безопасности, на примере КСОБЖН Ярославской области, обеспечивающей на базе единой сетевой телекоммуникационной и вычислительной инфраструктуры эффективное объединение всех существующих региональных и ведомственных подсистем безопасности в единую региональную информационно-техническую систему безопасности и существенное расширение их функциональных возможностей.

Детально рассматривается архитектура, принципы построения, структура единого мониторингового центра и регионального Ситуационного центра, обеспечивающих централизованный сбор, накопление, анализ информации о ситуации в регионе, а также принципы и их интеграции в инфраструктуру региональных центров управления, являющихся структурными подразделениями Национального центра управления обороной Российской Федерации и создаваемых на базе военных округов.

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

ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ РЕГИОНАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ

В последнее время в целях решения задач национальной обороны и обеспечения безопасности жизнедеятельности населения крайне актуальной стала задача создания комплексов технических средств и информационно-аналитических систем обеспечения региональной безопасности. Вместе с тем во многих регионах страны по инициативе различных министерств и ведомств (МВД, ФСБ, МЧС) уже созданы и функционируют различные системы обеспечения безопасности и противодействия ЧС. Однако они создавались в различное время, разными ведомствами, построены по различным принципам, что усложняет их дальнейшую интеграцию в единую систему. При этом основным инфраструктурным компонентом их интеграции должна стать единая мультисервисная высокоскоростная инфотелекоммуникационная сеть (МИТС), обеспечивающая объединение телекоммуникационных сетей (ТС) существующих ведомственных систем безопасности на основе единых защищенных протоколов и их интеграцию в единую инфраструктуру Региональных центров и Национального центра управления обороной страны.

В докладе рассматриваются принципы построения МИТС системы региональной безопасности, на примере МИТС КСОБЖН Ярославской области, обеспечивающей эффективное объединение ТС всех существующих региональных и ведомственных подсистем безопасности в рамках единой региональной информационно-технической системы безопасности.

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

ПРОБЛЕМЫ СОЗДАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ МОНИТОРИНГОВЫХ ЦЕНТРОВ, КАК ЭЛЕМЕНТОВ СИСТЕМ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

Современное развитие информационного общества характеризуется интенсивным внедрением автоматизированных информационных систем (АИС), направленных на повышение эффективности управления в том числе и городского (территориального) управления. Особое место среди задач информатизации в последний период стала занимать задача создания информационных систем сбора, накопления, анализа информации и поддержки принятия управленческих решений в области безопасности жизнедеятельности крупных мегаполисов и промышленных территорий, особо опасных объектов.

Вместе с тем, существует ряд проблем, сложившихся исторически и препятствующих повышению эффективности использования сетевых и информационных технологий в целом, которые носят комплексный межведомственный характер и не могут быть решены на уровне отдельных органов государственной власти.

Наиболее существенными из обозначенных проблем являются:

1. Результаты разработки и внедрения информационных технологий, проводящихся по заказу отдельных органов государственной власти, различных министерств и ведомств не всегда носят системный и скоординированный характер.

2. Реализуемые сетевые и технические решения, зачастую, ввиду ведомственной обособленности, носят дублирующий характер, что, в целом, затрудняет их совместное эффективное использование и приводит к нерациональному расходованию финансовых ресурсов.

3. Сохраняется высокий уровень различия в использовании информационных и сетевых технологий различными министерствами и ведомствами, отсутствует системный подход к построению комплексных региональных систем безопасности.

4. Отсутствуют проработки создания системообразующих информационных систем, обеспечивающих унифицированный доступ к функционально связанному, в рамках всех информационных систем или отдельных сфер жизни города, региона, набору услуг.

5. Отсутствие интеграции ведомственных региональных систем безопасности («Безопасный город», «Безопасный регион») с региональными центрами управления, являющимися структурными подразделениями Национального центра управления обороной Российской Федерации и создаваемыми на базе военных округов.

В докладе рассматриваются принципы построения системы региональной безопасности, на примере КСОБЖН Ярославской области, и ее основного элемента – Единого Мониторингового Центра, обеспечивающего на базе единой сетевой телекоммуникационной и вычислительной инфраструктуры эффективное объединение всех существующих региональных и ведомственных подсистем безопасности в единую региональную информационно-техническую систему безопасности, систематический сбор, кластеризацию, накопление и анализ информации о всех сферах жизнедеятельности региона.

Закалкин П.В., Кузнецов С.И., Сухорукова Е.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ЗАДАЧА МОНИТОРИНГА СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Несмотря на развитие рынка средств защиты информации, совершенствования систем управления инцидентами и событиями информационной безопасности (ИБ) – проблема защиты информационных систем остается актуальной. Зависимость от инфо-телекоммуникационных сетей (ИТКС) как отдельных индивидов, так и организаций растет с каждым днем, а вместе с этим увеличиваются потенциальные возможности нарушений реализованной политики безопасности. Об этом свидетельствует ежегодный рост неправомерных действий совершаемых в киберпространстве, таких как неправомерный доступ к обрабатываемой информации (банковских и кредитных карт, финансовой информации), создание и распространение вредоносных программ, массовая несанкционированная рассылка электронных сообщений любого характера и др.

Актуальность проблемы подчеркивается созданием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Необходимость создания данной системы назрела давно. Например, в США законодательное закрепление создания аналогичной системы FIDNET – федеральной сети обнаружения компьютерных атак – произошло в 1996 году, однако стоит отметить, что ее появление не принесло должного результата.

В существующих системах мониторинга можно выделить ряд ключевых недостатков.

Во-первых, данные системы не новы – основы их создания были заложены в начале 70 годов прошлого века, когда были созданы силы и средства по контролю над использованием радиочастот, техническими средствами связи и т.п.

Во-вторых, отсутствует указание на то, что в основе обнаружения, предупреждения и ликвидации последствий компьютерных атак находится система защиты информации, и она должна являться ключевым звеном.

В-третьих, используемый термин компьютерные атаки не включает весь спектр возможных нарушений, предлагается использовать вместо него два термина, а именно техническая компьютерная разведка (ТКР) и деструктивные средства воздействия (ДСВ).

В-четвертых, как правило, ДСВ направляются не только на информационные ресурсы, но и на всю ИТКС в целом.

С учетом современного развития ИТКС и возможностей нарушителей, статические (неизменные) системы защиты информации (СЗИ) становятся малоэффективными. Возникает необходимость создания динамической системы защиты информации позволяющей оперативно подстраиваться под быстроизменяющиеся условия функционирования объекта защиты. Необходимым условием реализации динамических систем защиты является наличие эффективной системы мониторинга, которая:

1. предоставляет информацию о возможностях нарушителя и реализуемые им стратегии действий;

2. фиксирует источники, время и место реализации, тип и средства деструктивного воздействия;

3. выявляет объективные демаскирующие признаки ИТКС и оценивает их информативность, время и место проявления, и среднее время существования.

Необходимо учитывать, что в современных ИТКС реализация мер защиты является достаточно длительным по времени процессом. Соответственно, при большом времени мониторинга и принятия решения, времени на оперативную реализацию мер защиты практически не остается. Что позволит нарушителю ИБ провести разведку и реализовать ДСВ. Таким образом, для оперативного реагирования под быстроизменяющиеся условия функционирования объекта защиты – необходимо решить задачу оптимального (рационального) распределения ресурсов на подсистемы мониторинга, принятия решения, реализации мер защиты.

Закалкин П.В., Сухорукова Е.В., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ЗАЩИТА НАЦИОНАЛЬНОЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ КИБЕРВОЗДЕЙСТВИЙ

Стремительное развитие информационных технологий и глобализация Интернета привели к тому, что элементы национальной критической инфраструктуры (НКИ) становятся объектом преступной деятельности, появляется больше «мишеней» для противоправных посягательств, преступные и террористические группы получили возможность использования глобальной сети в своих преступных намерениях.

Исследования критической инфраструктуры становятся приоритетными во многих странах мира, и в первую очередь в США, где уровень развития информационных технологий и возможности современных комплексов имитационного моделирования постоянно повышаются. Наибольшую обеспокоенность США вызывает потенциальная возможность скрытного кибервоздействия на объекты критических инфраструктур ключевых секторов экономики, от состояния которых зависит безопасность страны и общества (энергообеспечение, водоснабжение, транспорт и др.), с целью нарушения их работоспособности или вывода из строя.

Помимо этого 19 мая 2013 года было обнародовано разработанное объединенным центром передового опыта по кибероборонe НАТО (Cooperative Cyber Defense Center of Excellence, CCD COE) руководство о применении положений существующего международного права к кибервойнам. Документ под названием "Таллиннское руководство по ведению кибервойн" объемом в 300 страниц содержит алгоритмы действий государств и военных альянсов на случай более масштабных атак.

Таким образом, задача защиты национальной критической инфраструктуры становится основополагающим аспектом общественной безопасности и экономической стабильности. При этом необходимо обеспечивать защиту как от преступных и террористических групп, так и от целенаправленных кибероперaций зарубежных стран.

Проведение подобных кибероперaций потребует информации о используемых средствах защиты, порядке функционирования объектов и т.д.. В результате атаки помимо нарушения функциональности, возможна утечка информации о новейших используемых (проходящих испытания) разработках, а в области полезных ископаемых и нефте-газовой отрасли возможна утечка данных о стратегических запасах, о резервных хранилищах и законсервированных разработках, а так же об условиях залегания, оставшемся ресурсе и объемах выработки на действующих месторождениях.

Все НКИ разные, но общим для них является необходимость обеспечения защиты информации. Утеря информации, кратковременное предоставление её в открытый доступ и т.д. и ее последующее использование зарубежными государствами или террористическими группами может привести к непредсказуемым последствиям.

Одним из вариантов защиты новой информации является патентование в федеральной службе по интеллектуальной собственности (Роспатент), однако РФ не со всеми странами имеет договоры о признании патентного права.

Для организации эффективного противодействия несанкционированным действиям в киберпространстве, направленных против НКИ необходимо:

– Выявление и каталогизация уязвимостей защищаемых объектов.
– Разработка средств, систем и способов защиты информации
– Создание условий для регулярного уточнения перечней угроз.
– Разработка моделей угроз.
– Создание новых специальностей, подготовка высококвалифицированных кадров обеспечивающих безопасность киберпространства.
– Детальное исследование и формализация аспектов противоборства в киберпространстве.
– Создание нормативно-правовой базы законодательно определяющей действия в киберпространстве.

Зегжда Д.П., Зегжда П.Д., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехническийуниверситет Петра Великого

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ ПРИ ПОСТРОЕНИИ ОТЕЧЕСТВЕННОЙ УНИВЕРСАЛЬНОЙ ЗАЩИЩЕННОЙ СЕТЕВОЙ УПРАВЛЯЮЩЕЙ ПЛАТФОРМЫ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРУПНОМАСШТАБНЫХ СЕТЯХ С ДИНАМИЧЕСКОЙ ИНФРАСТРУКТУРОЙ

Задача создания отечественных универсальных защищенных сетевых управляющих платформ вызвана необходимостью импортозамещения, потребностью в надежных, производительных и защищенных средствах управления большими сетями с динамической инфраструктурой, устойчиво функционирующих в условиях изменяющейся картины угроз. Такая платформа должна решать задачу универсализации способов управления сетевым оборудованием;обеспечивать интеллектуальное управление сетевыми потоками с возможностью виртуальной сегментации сетей в зависимости от их назначения, топологии, правил маршрутизации, политик безопасности (взаимодействующих сервисов и объектов);реализовывать принципы автоматического управления, разграничения и контроля информационных потоков в компьютерной сети с изменяемой инфраструктурой;повышать защищенность и отказоустойчивость сетевого оборудования и систем управления сетевым оборудованием.

Такая платформа создана авторами на базе технологии программно-конфигурируемых сетей (ПКС, Software Defined Networks, SDN) и включает легковесное виртуальное окружение на высокопроизводительном серверном оборудовании и сервисы поддержки управления сетевыми потоками (прокси-слой и виртуальные экземпляры программных систем управления ПКС).Платформа реализует функции автоматизации многослойного, мультисервисного управления сетью и виртуализации сетей, позволяя множеству логических сетей сосуществовать на общей физической сетевой топологии. С этой целью реализуется программный прокси-слой между OpenFlow-коммутатором и виртуальными контроллерами ПКС, который на базе характеристик входящего трафика и информации о состоянии узлов ПКС, истории обработки сетевых потоков, статистики, текущего уровня нагрузки, требований по безопасности и прочих управляющих параметров определяет, какому сетевому слою (срезу, в терминологии ПКС) сети принадлежит данный трафик и сопоставляет соответствующий виртуальный контролер ПКС.

В платформе реализована система потоковых сервисных пространств: множество потоков трафика в каждом выделенном слое образуют свое потоковое сервисное пространство. На базе предложенного решения реализуется пользовательский программный интерфейс конструирования и автоматического создания множества изолированных виртуальных сетевых топологий поверх физической ПКС. Оператор, создавая политику разграничения слоев, визуально конструирует сетевые срезы в зависимости от политики организации или функциональных ограничений с учетом доменов субъектов и объектов взаимодействия. Затем применяет данную политику к физической топологии ПКС, реализуя на OpenFlow-коммутаторе виртуальную сегментацию на логические подсети. В данном случае платформа представляет собой логическую точку защиты (ЛТЗ), т.е. реализует концепцию программно-конфигурируемой безопасности, согласно которой контроллер ПКС отвечает за логическую группу узлов ПКС и позволяет сгенерировать необходимые OpenFlow-правила, привязав тип трафика к соответствующему слою (срезу) сети для изолированной обработки.

Данное решение применимо для сетей с динамически изменяемой инфраструктурой (включая «Интернет вещей», «туманные» системы, mesh-сети) любой сложности, поскольку поддерживается наращивание мощностей за счет распределения функций управления между несколькими виртуальными контроллерами ПКС и сопряжения множества платформ.

Достоинства такого решения:

– открытость платформы;
– унификация интерфейса управления сетевым оборудованием на базе протокола OpenFlow;
– независимость от производителей оборудования;
– повышение безопасности, улучшение контроля и мониторинга событий безопасности и состояний сетевого оборудования;
– облегчение сертификационных исследований.

Эффект от использования технологии ПКС при построении отечественных защищенных сетей заключается в следующем. Число аппаратных и программных компонентов, выполняющих различные функции управления, сокращается до минимума вследствие переноса функций управления на уровень контроллера ПКС. Сертификационные исследования ПКС-коммутаторов в значительной степени облегчаются по причине наличия открытых исходных кодов на всех уровнях системы (оборудование, протокол, контроллер ПКС). Функции мониторинга безопасности выполняются средствами контроллера ПКС. Полная независимость от производителя сетевого оборудования за счет переноса управления на программный уровень контроллера ПКС в значительной мере повышает гибкость и эффективность управления, а также уровень сетевой безопасности.

Израилов К.Е.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича

ПОИСК УЯЗВИМОСТЕЙ В РАЗЛИЧНЫХ ПРЕДСТАВЛЕНИЯХ ПРОГРАММНОГО КОДА

Несмотря на неослабевающую актуальность поиска уязвимостей в программном коде устройств для всех области, одной из наиболее приоритетных считается телекоммуникационная. Во-первых, это следует из того, что основным предназначением телекоммуникационных устройств является обработка информации, которая зачастую является конфиденциальной. А, во-вторых (что особенно актуально для России), такие устройства поставляются зарубежными производителями без исходного кода – только в виде машинного, что значительно затрудняет анализ кода и последующий поиск.

Перед разработкой методов поиска уязвимостей необходимо четкое понимание причин их появления – как случайных, так и злонамеренных. А с учетом того, что программный код от самого зарождения до окончательной загрузки в рабочее устройство пребывает в различных представлениях, то необходимо учитывать возможности появления уязвимостей в каждом из них. Такое понимание, в частности, позволит выбирать и использовать максимально подходящие способы поиска уязвимостей для каждого представления.

Типичные для телекоммуникационного устройства поэтапные преобразования программного кода в процессе создания конечного продукта проходят через следующие представления; при этом форма представления может быть различной – текстовой, бинарной, в виде блок-схем. Вначале возникает мысленный прообраз кода, отражающий основную идею и описывающий требуемый функционал, характеристики, свойства. Уязвимости в таком прообразе отсутствуют, поскольку на данном этапе невозможно их отличить от особенностей самой идеи.

Используя прообраз, разрабатывается концептуальная модель, вводящая основные понятия, их структуру, взаимосвязь и т.п. В этот момент уже возможно возникновение уязвимостей в виде принципиальных различий созданной модели и первоначальной идеи.

По концептуальной модели разрабатывается архитектура кода, приближенная к будущей реализации; в частности, архитектура может содержать конкретные технологии, парадигмы языков программирования, форматы данных. Ошибки в проектировании архитектуры также приведут к наличию уязвимостей в программном коде. Используя архитектуру, создаются алгоритмы работы ее функционала.

Данный процесс носит творческий характер, что как неизменно связано с появлением в схеме алгоритма случайных ошибок, так и успешно используется для внедрения злонамеренной логики, например программных закладок. Созданные алгоритмы, как правило, переписываются в виде операций на заданном архитектурой языке программирования, создавая так называемый исходный код программы. При достаточной степени детализации алгоритмов и аккуратности выполнения программистом кодирования случайных ошибок можно избежать; тем не менее, на данном этапе возможно (и успешно применяется) внесение в код злонамеренных уязвимостей, хотя и имеющих менее абстрактный уровень, чем в предыдущем представлении.

Далее исходный код преобразуется в ассемблерный с помощью специальных утилит – компиляторов. Возникновение в результате ошибок в инструкциях процессора носит лишь теоретический характер, поскольку это возможно вследствие неверной работы таких утилит, что маловероятно. Машинный код программы получается из ассемблерного в общем виде тривиальным преобразованием инструкций процессора из записанных в текстовом виде в соответствующий им бинарный. Возникновение уязвимостей в этом представлении, аналогично ассемблерному, практически невозможно. Для загрузки на конечное телекоммуникационное устройство выполнение, машинный код, как правило, собирается в единый файл образа, также без каких-либо новых уязвимостей.

Согласно приведенным представлениям можно сделать следующие выводы. Во-первых, преобразования понижают абстрактность используемых в представлениях элементов – от общей идеи через пошаговые алгоритмы до инструкций процессора. Во-вторых, уязвимости могут появляться в различных представлениях, притом имея соответствующий структурный уровень (тип) согласно их абстрактности в программном коде – уязвимости в концептуальной модели и архитектуре (высокоуровневый), алгоритмах (среднеуровневый) и их реализации через операции (низкоуровневый). И, в-третьих, возникшая уязвимость в одном представлении существует и во всех последующих, поскольку происходит лишь ее «размывание» по программному коду. В

се это позволяет утверждать, что поиск уязвимостей каждого типа целесообразно производить по представлению, строящемуся на элементах соответствующего уровня абстракции. В случае же наличия для поиска только машинного кода, обозначенные для поиска представления необходимо из него получить. Также возможным решением может быть получение объединенного представления для поиска всех трех типов уязвимостей.

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

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

За последние два десятилетия обеспечение информационной безопасности автоматизированных систем стало самостоятельным направлением развития современных информационных технологий. Наглядным подтверждением этому стало появление специализированных международных институтов, занимающихся проблемами защиты информации; открытых стандартов на технологии обеспечения ИБ; законодательной базы, регулирующей вопросы построения систем защиты информации (СЗИ); специализированных продуктов и решений по защите информации и т.д.

Построение многокомпонентных систем защиты информации в большинстве случаев не является современным решением проблемы информационной безопасности автоматизированных систем специального назначения. Проектирование комплексной (в широком смысле этого слова) системы защиты информации является достаточно сложной системно-аналитической задачей, которая требует специальной и достаточно строгой методики. Предлагаемые известными российскими и международными институтами методики (ФСТЭК России, ISO и др.) в большинстве своем носят общий характер.

Предлагаемая методика носит открытый характер и может быть полезна в качестве инструмента выработки технических требований и контроля корректности построения необходимой системы защиты.

Поскольку любая система СЗИ в конечном итоге должна «накладываться» на реальную информационную систему, для ее описания целесообразно было бы использовать многоуровневую иерархическую модель.

Одним из главных преимуществ представления системы защиты информации в виде иерархии функционально-независимых уровней является существенное упрощение процесса проектирования системы.

Предлагаемый пятиуровневый подход помимо упрощения самого процесса проектирования, позволяет четко формализовать три достаточно сложные задачи, которые неизбежно возникают при создании систем защиты автоматизированной системы специального назначения:

– обеспечение целостности (комплексности) системы защиты;

– разграничение требований и функций системы защиты информации при защите информации, обладающей различной степенью конфиденциальности;

– обеспечение целостности системы защиты информации при защите территориально-распределенных информационных систем.

Защита всех трех разновидностей информационных ресурсов в рамках одной и той же СЗИ подразумевает, что даже открытые ресурсы будут защищаться по требованиям, предъявляемым к защите информации ограниченного доступа, что приведет к необоснованно высокой стоимости СЗИ и неудобствам работы для сотрудников. Так же неэффективно будет построение трех различных СЗИ для каждого из ресурсов, так как четко разделить эти ресурсы в рамках одной АС СН практически невозможно и это также приведет к повышению стоимости самой системы защиты.

В рамках предложенной модели указанная проблема может быть решена путем разграничения требований и, соответственно, функциональности для каждого из уровней защиты СЗИ применительно к каждой группе информационных ресурсов.

В заключение можно подчеркнуть, что предлагаемый подход к проектированию СЗИ на базе иерархической пятиуровневой модели носит методический характер. Тем не менее, такой системный подход позволяет существенно сократить сроки разработки системы защиты информации и при этом выработать действительно оптимальное и обоснованное решение.

Калинин М.О., Минин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ В MESH-СЕТЯХ С ПОМОЩЬЮ АЛГОРИТМОВ SOFT COMPUTING

Широкое распространение мобильных технологий, возрастающая популярность «Интернета вещей» и «умного дома» привели к появлению одноранговых сетей с динамически изменяемой топологией (mesh-сетей). Число устройств, образующих такие сети, может быть огромным, и оно постоянно изменяется. Также эти устройства могут постоянно перемещаться, поэтому классические подходы организациисетей для них неприменимы. В mesh-сетях применяется одноранговая маршрутизация, в которой таблицы маршрутизации формируются самими узлами сети, основываясь на метриках соединений. Имитируя лучшую метрику, узел-нарушитель может намеренно

переориентировать сетевые потоки, в связи с чем при выборе безопасного маршрута необходимо учитывать не только метрику соединений, но и уровень доверия к узлу.

Устройства в mesh-сети чаще всего маломощные, поэтому применять в них классические средства защиты информации, такие как антивирусные средства и межсетевые экраны, невозможно. Применение централизованных средств защиты также неэффективно, так как информация на центральном узле может быстро устаревать и не совпадать с тем, что есть в действительности. Средства безопасности в mesh-сетях должны удовлетворять следующим критериям: масштабируемость, гибкость, адаптивность. Таким критериям удовлетворяют системы безопасности, основанные на алгоритмах семейства «softcomputing», в частности роевых. Важным преимуществом таких алгоритмов является непрямое взаимодействие между агентами в сети, а взаимодействие посредством феромона, что позволяет уменьшить нагрузку на сеть.

Устройства в одноранговой сети часто имеют множество соединений с другими устройствами, и, как следствие, множество маршрутов до одной точки назначения. Для выбора безопасного маршрута вводится понятие доверия к узлу. Для расчета доверия к узлу применяется муравьиный алгоритмsoftcomputing. Все узлы сети рассылают специальные пакеты трассировки, не отличимые от обычного трафика, на различные узлы сети через различные соединения. Если на отправленный пакет получен ответ, то количество феромона на этом соединении увеличивается в зависимости от скорости ответа, что позволяет отличить быстрые доверенные соединения от медленных. Если ответ не был получен, то часть феромона для этого соединения удаляется.

Использование алгоритмов softcomputingпозволяет со временем перестраивать доверенный маршрут из узлов сети, которые гарантированно передают трафик, и тем самым избегать узлов, которые не передают трафик или выполняют некорректную маршрутизацию в сети.

Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ ВИРТУАЛЬНЫЙ КЛАСТЕР КАК УНИВЕРСАЛЬНАЯ ПЛАТФОРМА ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ШИРОКОПОЛОСНЫХ СЕТЯХ

Сложность решения задач обеспечения информационной безопасности в современных сетях широкополосного доступа к мультимедийным данным заключается в том, что внедрение и работа средств защиты информации (СЗИ) существенно влияет на интегральную производительность систем безопасности вследствие увеличения потребления вычислительных ресурсов и понижения пропускной способности сетевой подсистемы.

Для решения данной проблемы предлагается реализовать программные компоненты СЗИ, выполняющие обработку сетевого трафика, на виртуальных машинах, работающих на базе вычислительного кластера (суперкомпьютера). С целью повышения производительности используются несколько идентичных экземпляров программных модулей СЗИ.

Основу для балансировки входящей сетевой нагрузки составляет разработанный метод классификации потоков сетевого трафика, заключающийся в выделении сетевых потоков на основе ключевых характеристик (например, IP-адресов и портов источника/назначения). Таблица потоков применяется для демультиплексирования входящего потока трафика на потоки, предназначенные конкретному узлу.

Этапы реализации высокопроизводительных СЗИ для систем предоставления широкополосных цифровых мультимедийных услуг:

– входящий сетевой трафик попадает на балансировщик нагрузки, который распределяет входящий трафик по узлам виртуализированного вычислительного кластера;

– в каждом узле СЗИ выполняют обработку каждого проходящего IP-пакета, оставляя IP-заголовок для сохранения маршрутизации;

– после обработки трафик поступает на выходной сборщик потоков.

Разработанное решение обеспечивает обработку трафика с пропускной способностью до 10 Гбит/с. Кластерное решение позволяет добиться следующих конкурентных преимуществ:

– выделение СЗИ в отдельный сетевой компонент, что позволяет избежать необходимости адаптации системы;

– распараллеливание вычислительных процессов, что повышает эффективность и скорость обработки сетевого трафика;

– применение балансировки нагрузки, благодаря чему повышается отказоустойчивость СЗИ;

– сокращение расходов на обслуживание ввиду прозрачности системы и повышение надежности;

– масштабирование вычислительной мощности на выделенном сервере за счет динамического изменения пула виртуальных машин, что экономически более эффективно, чем группы физических серверов.

Внедрение данного решения в системы массовых цифровых услуг позволяет уменьшить загруженность серверов приложений и обработки данных за счет централизации функций защиты на

одном физическом сервере с поддержкой параллельной обработки трафика и тем самым повысить эффективность использования таких систем, обеспечивая требуемый уровень безопасности при повышении интегральной пропускной способности сетевой подсистемы защиты.

Кий А.В., Логинов В.А., Лощенин Д.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБ ИЗБЫТОЧНОСТИ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ПОДХОДЕ К ЕЕ СНИЖЕНИЮ

Возможности пользователя по подготовке и совершению НСД в значительной степени определяются множеством предоставленных в доступ информационных ресурсов автоматизированной системы (АС) и множеством полномочий по доступу к ним, которые, как правило, являются избыточными по отношению к выполняемым пользователями функциональным задачам. Причиной возникновения избыточности является асимметричность решений при назначении полномочий. Если невозможно точно определить минимальный набор полномочий, достаточный для выполнения задач пользователем, то решение принимается в пользу некоторого добавления прав, иначе может быть нарушена функциональность АС. Это утверждение справедливо также и по отношению к учетным записям служб и приложений. Другой причиной избыточности полномочий пользователей является статичность моделей управления доступом, которые не учитывают периодичность использования тех или иных полномочий. Это приводит к тому, что вне зависимости от текущего содержания деятельности пользователя ему постоянно предоставлен весь объем ранее запланированных полномочий.И, наконец, ошибки администрирования, связанные с дефицитом времени, значительным числом пользователей АС и недостаточным уровнем подготовленности администраторов безопасности, осуществляющих разработку и ввод в систему правил разграничения доступа.

Таким образом, можно утверждать, что реально предоставляемые полномочия всегда избыточны по отношению к объективно необходимым. При этом следует констатировать наличие как априорной, так и контекстной избыточности.

Априорная избыточность характеризует превышение предоставленных пользователю при разграничении доступа полномочий относительно реального объема, необходимого для решения возложенных на него задач.

Контекстная избыточность характеризует превышение предоставленного объема полномочий относительно реальных потребностей пользователя в контексте отдельной функциональной задачи.

В качестве показателей априорной и контекстной избыточности полномочий пользователя предложены соответствующие коэффициенты априорной и контекстной избыточности.

Результаты оценки контекстной избыточности полномочий пользователей, проведенные на основании исходных данных, полученных с помощью программ AccessChk и Process Monitor, входящих в состав набора программ Sysinternals Suite, показывают, что в ряде случаев коэффициентконтекстной избыточности достигает 0,9, что не может не беспокоить специалистов в области безопасности информации.

Если рассматривать каждый запрос пользователя по доступу к ресурсу, не относящемуся к перечню ресурсов необходимых для выполнения задачи, как ошибочный или подготовку несанкционированного доступа (НСД), даже в том случае, если данное действие в явном виде не нарушают принятую политику безопасности, и не ограничивать его в совершении таких действий, то вероятность НСД, будет расти и может достигнуть предела допустимого значения.

Решить данную проблему может применение механизма адаптивного разграничения доступа, основанного на динамическом формировании частных схем разграничения доступа (СРД), соответствующих текущим задачам пользователя. Переключение между формируемыми частными СРД осуществляется на основании сравнения их идентификаторов и идентификаторов функциональных задач пользователя.

Ковриченков С.В., Кузнецов С.И., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ

Учитывая интеграцию информационно-телекоммуникационной сети военного назначения (ИТКС ВН) с системой связи общего пользования (ССОП), очевидной становится возможность вскрытия элементов ИТКС ВН (построения ее адресной структуры), а также воздействия программными средствами через ССОП.

Существующие методы обеспечения безопасности с помощью «защитных оболочек» не всегда эффективны и легко подвержены воздействиям. Это связано с тем, что элементы ИТКС ВН легко

обнаруживаются. Это позволяет констатировать проблему, заключающуюся в разработке механизмов обеспечения скрытности адресного пространства ИТКС ВН на фоне ее элементов.

Анализ известных решений, позволили сделать выводы, что обеспечение скрытности возможно за счет управления характерными признаками ИТКС ВН. На структурном уровне система, обеспечивающая скрытность информационного обмена в ИТКС ВН не должна отличаться от системы, представленной в ИТКС ВН. Искусственная смена адресов дает возможность изменять видимую структуру распределенной ИТКС ВН, добавляя в нее новые элементы и связи между ними, создавая, таким образом, видимость ложной структуры, состоящей из большего количества элементов и множества связей между ними. Причем за счет смены адресов новые элементы ИТКС ВН не будут ложными, а информационный поток, реализующий информационный обмен между элементами будет разбиваться на совокупность информационных потоков.

Предлагаемый способ обеспечивает повышение безопасности и скрытности работы ИТКС ВН за счет усложнения процедуры определения адресов и выявления взаимосвязей удаленных сегментов при анализе трафика в некоторой точке ССОП путем непрерывного изменения в передаваемых пакетах сообщений адресов отправителя, адресов получателя в выделенном диапазоне и передачи пакетов многопоточно по различным маршрутам через транзитные пункты, использующие локальный сегмент защиты, что делает практически невозможным определение и идентификацию пакетов относительно конкретного пользователя сети, вскрытие структуры ИТКС ВН или определение направления информационного обмена.

Способ заключается в использовании локального сегмента защиты (ЛСЗ). Назначения IP-адреса из возможного диапазона на ограниченное время, называемое временем аренды и возможность впоследствии повторно использовать этот IP-адрес для назначения другому абоненту на основе информации о нем, полученной от корреспондента. При установлении соединения новым корреспондентом сети используется сервер со статическим IP-адресом, предоставляющий подключившемуся вновь ЛСЗ информацию о текущих динамических адресах взаимодействующих ЛСЗ. Поток сообщений от отправителя до получателя равными долями разбивается на N потоков. При обмене пакетами сообщений происходит динамическое изменение адреса отправителя и получателя. Полученные временные адреса включаются в зарезервированные сектора блока. Кодирование блока данных обеспечивает сохранность обратных адресов. Санкционированность информационного обмена подтверждается расчетом хэш-функции от поля данных пакета, с использованием индивидуального ключа для каждого ЛСЗ, и проверкой ее достоверности в каждом ЛСЗ.

Таким образом, вероятность определения нарушителем истинной структуры ИТКС ВН уменьшается, т.к. для такого определения необходима реконструкция трафика сети и длительное время, аналитические исследования, за которое топология построения скрываемой нами сети изменится, уменьшается вероятность обнаружения каналов связи удаленных сегментов ИТКС ВН. Следовательно, вероятность осуществления деструктивных воздействий значительно снизится, т.е. обеспечивается возможность достижения сформулированного технического результата – повышения безопасности ИТКС ВН.

Ковриченков С.В., Кузнецов С.И., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

НАПРАВЛЕНИЯ СОЗДАНИЯ ЕДИНОГО МЕХАНИЗМА БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ

Совершенствование форм и способов вооруженной борьбы, высокий уровень информационного обеспечения боевых действий войск (сил) становятся определяющими факторами достижения стратегического и оперативно-тактического превосходства над противником. Перевод системы связи ВС РФ на цифровое оборудование расширяет возможности противника для ведения информационной борьбы и требует повышения требований по безопасности информационно-телекоммуникационной сети военного назначения (ИТКС ВН). Необходимость обеспечения безопасности ИТКС ВН требует поиска качественно новых подходов к решению многих технических и управленческих задач.

Одним из слабых звеньев в вопросах обеспечения безопасности ИТКС ВН является использование на УС комплексного оснащения в качестве пограничных устройств маршрутизаторов зарубежного производства, которые используются и как средства обеспечения безопасности, препятствующие прозрачному взаимодействию между узлами разных подсетей ИТКС ВН.

Их применение является той уязвимостью, которую можно использовать для нарушения работы ИТКС ВН или циркулирующей в ней информации. Т.е. маршрутизатор является тем уязвимым компонентом ИТКС ВН, который наиболее подвержен к угрозам.

Одним из подходов и направлений обеспечения безопасности ИТКС ВН должно являться создание маршрутизаторов отечественного производства, которые будут являться встроенными

элементами единого самозащищающегося механизма безопасности ИТКС ВН. Эта стратегия даст возможность не только своевременно выявлять и предотвращать угрозы безопасности ИТКС ВН, но и противодействовать им. Единый самозащищающийся механизм безопасности ИТКС ВН должен быть построен на базе систем интегрированной безопасности, коллективной безопасности и адаптивной защиты.

При создании механизма интегрированной безопасности ИТКС ВН центральными элементами в системе должны выступать маршрутизаторы. В них должны найти отражение такие функции как, обеспечение надежного и масштабируемого сетевого взаимодействия, включая различные типы трафиков, предотвращение сетевых атак и угроз, и применение против них ответных мер, используя сетевые сервисы, применение в сети интеллектуальных механизмов защиты конечных узлов с использованием таких технологий, как аутентификация, авторизация и аудит, инфраструктура открытых ключей и сервисы идентификации.

Создание системы коллективной безопасности (общесетевой), должно охватывать конечные узлы, сеть и правила политик ИТКС ВН (контроль доступа в сеть, где сервисы и устройства скоординировано, отражают атаки благодаря активному управлению доступом). Она должна включать в себя анализ угроз в динамике на различных уровнях, помогая ужесточить контроль над сетевым трафиком, конечными точками, пользователями и приложениями.

Создание адаптивной защиты должно быть реализовано на основе высокопроизводительных решений надежной многоуровневой интеллектуальной логики, защиты приложений, контроля в масштабах всей сети и локализации угроз, с учетом защиты сетевой инфраструктуры от атак и угроз, особенно на уровне сети.

Также требуется предусмотреть создание менее сложной архитектуры и снижение операционных расходов, за счет размещения сервисов на меньшем количестве устройств, более скоординированной системы нейтрализации угроз.

Создание механизма интегрированной безопасности ИТКС ВН, позволит превратить в оборонительный рубеж защиты каждый сетевой элемент, в том числе маршрутизаторы, коммутаторы, встраиваемые модули и конечные узлы.

Кораблин В.О.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

ОПЕРАТИВНАЯ ОБРАБОТКА ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИЙ

При построении интегрированной системы оценки информационной безопасности гетерогенной информационной или телекоммуникационной системы особое внимание следует уделить информационному взаимодействию с различными источниками данных.

Предоставляемые источниками данных сведения потенциально имеют различные форматы представления, что затрудняет их централизованное хранение в некотором хранилище данных. Также имеется некоторая избыточность данных по отношению к системам оперативного контроля информационной безопасности.

Для уменьшения передаваемых данных и оптимизации нагрузки на сети передачи, необходимо создать средства сбора и предварительной обработки данных, минимизирующих передаваемые объемы.

При наличии таких средств, появляется возможность осуществлять сбор данных и их предварительную обработку, например, переводя их из одного подмножества значений в другое на основе сформулированных правил пересчета. Так например из множества поступающих сведений от средств защиты может быть сформировано определенное множество событий, которые агрегируют полученные данные. Дальнейшая обработка событий информационной безопасности заключается в определении степени угрозы защищаемой системе.

Программные средства, осуществляющие сбор и обработку данных (событий) информационной безопасности должны иметь гибкий адаптационный механизм, формируемый на основе трех принципов:

1. Динамически подключаемые программные модули;
2. Метауправление сбором данных;
3. Конфигурирование средства сбора данных.

Наличие динамически подключаемых программных модулей, осуществляющих взаимодействие с конкретными типами источников данных, позволяет упростить и ускорить внедрение системы, обеспечить мониторинг любых типов источников данных.

Мемтауправление дает возможность оперативно изменять набор собираемых и обрабатываемых параметров источников данных, уменьшая нагрузку на средства обработки. Оптимальным является минимальный необходимый и достаточный для полного отображения состояния безопасности телекоммуникаций набор обрабатываемых параметров.

Предварительная обработка должна осуществляться в интересах уменьшения нагрузки на сеть, ухода от избыточности данных и оптимизации представления данных. Также возможно значительное упрощение процедуры обработки данных при переходе от количественных значений качественным показателям, например, осуществляя свертку, переходя от количественных значений к качественным показателям, описываемым логическими значениями принадлежности значения параметра задаваемому диапазону. Наличие механизма предварительной обработки позволяет оптимизировать обнаружение критических состояний параметров безопасности.

Таким образом, представленный подход построить подсистему оперативного сбора и хранения данных событийного мониторинга в интересах средств информационной безопасности.

Корниенко Е.А., Кревная А.И., Стародубцев Ю.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

О ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

В настоящее время сложилась ситуация, которая принципиально изменяет традиционный порядок создания и последующего развития информационно-телекоммуникационных систем (ИТКС), а соответственно способов и методов защиты информационных ресурсов.

Суть традиционного подхода к созданию ИТКС заключалась в выполнении следующей последовательности действий: определение объекта управления; создание (синтез) системы управления; формирование требований к ИТКС и,собственно, формирование ИТКС, соответствующей заданным требованиям.

Вопросы защиты информационных ресурсов решались на основе принципов физической и логической изолированности систем связи конфликтующих систем управления. Более того, в каждой системе управления элементы ранжировались по важности, а вокруг них развертывались контролируемые зоны.

Контролируемая зона, в классическом понимании, определялась как пространство, в пределах которого исключается неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств

К настоящему времени можно констатировать, что создана и продолжает развиваться общемировая единая информационно-телекоммуникационная система (ОМЕИТКС), в связи с чем неуклонно сокращается число систем управления, опирающихся на уникальные (собственные) системы связи.

Однако самостоятельное и неконтролируемое со стороны любой выделенной системы управления развитие общемировой единой информационно-телекоммуникационной системы существенно изменяет условия обеспечения защиты информационных ресурсов.

Во-первых, предположения о полной априорной известности характеристик (параметров) объекта защиты не соответствует сложившейся ситуации.

Во-вторых, предположение о необходимости первоочередной защиты органов управления и соответствующих им элементов ИТКС требует серьезного переосмысления.

В-третьих, принцип равнопрочной защиты всех взаимодействующих элементов представляется избыточным и неэффективным.

В-четвертых, обеспечение равноправной защиты всех элементов в течение всего времени функционирования системы управления вызывает сомнения.

Это далеко не полный перечень условий и принципов организации и обеспечения защиты информационных ресурсов, требующий пересмотра.

Объектами воздействия в сложившихся условиях могут быть не столько органы управления, сколько совокупность реализуемых процессов (функций).

Принципиально изменился и вид угрозы. Если в традиционном варианте это человек (группа лиц), либо техническое средство, то в сложившейся ситуации это программный агент, воздействующий либо на логику защищаемого процесса, либо на характеристики инфокоммуникационной среды его реализации. В настоящее время угрозы характеризуются:относительной невидимостью; высоким быстродействием;существенным расширением множества точек возможных реализаций;значительной величиной скрытого периода.

В этой связи необходимо осуществить переход к созданию многорубежных систем защиты применительно к элементам телекоммуникационной среды развития конфликта.

Основной целью является временное, динамично изменяемое выделение и контролируемое использование части общего телекоммуникационного пространства для реализации совокупности реализации процессов (технологических процедур) управления. При этом может возникнуть потребность во временном контроле параметров (характеристик) элементов системы связи общего пользования и удержание (изменение) их в желательном состоянии.

Кочкин В.А., Хилько В.О., Аксенов С.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СИСТЕМЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ С ГИБРИДНОЙ РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ

В последние годы услуги по передачи данных получили наибольшее развитие и распространение в Вооруженных Силах Российской Федерации. Должностные лица уже не удовлетворяются просто наличием связи, им требуются гарантированные скорости передачи, задержки и показатели верности передачи. Рост объёмов передаваемой информации в сетях передачи обуславливает необходимость разработки систем, наиболее эффективно использующих пропускную способность каналов. Наибольший интерес в настоящее время имеют беспроводные каналы связи имеющие нестационарный характер. При этом возникает проблема выбора способов и систем передачи, которые обеспечат требуемые качественные показатели в заданных условиях с минимальными затратами. В современных условиях применение гибридной решающей обратной связи позволяет повысить качественные показатели систем передачи данных.

Системы передачи данных с гибридной решающей обратной связью занимают промежуточное положение между системами с переспросом и системами с прямым исправлением ошибок, комбинируя лучшее из этих двух стратегий. Идея состоит в переспросе не только информационной последовательности, как это делается в классических системах передачи данных, а так же последовательности проверочных элементов кода с высокой исправляющей способностью, что позволяет снизить затраты на передачу одного бита информации и повысить производительность системы.

В научных трудах вопросами анализа систем с гибридной решающей обратной связью занимались Е. Высоцкий, О.Г. Мелентьев, Shu Lin, Michael Miller, Fulvio Babich, Robert Deng, Masao Kasahara, Samir Kallel и другие.

В настоящее время системы повышения достоверности с гибридной решающей обратной связью используются в стандарте UMTS и активно внедрены в стандарты мобильной связи, такие как 3GPP Long Term Evolution (LTE) и IEEE 802.16 (WiMAX). Однако до сих пор отсутствуют практические рекомендации по использованию различных вариантов систем с гибридной решающей связью.

Таким образом, системы с гибридной решающей обратной связью в зависимости от используемого корректирующего кода позволяют в разной мере повысить верность доставки и эффективность использования канала в сравнении с классической системой с решающей обратной связью.

КоцынякМ.А., ЛаутаО.С., ШаровИ.А., Сабан М.Ю., ХорошковМ.Э.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПЕРСПЕКТИВНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И СВЯЗИ И ПУТИ ИХ СОЗДАНИЯ

При наличии автоматизированных комплексов связи правомочна постановка задачи на синтез оптимальной системы управления и связи в условиях многофакторного воздействия. Для решения такой задачи целесообразно использовать принципы системного подхода, учитывающие внешние параметры (требования Заказчика) и внутренние параметры – параметры комплексов связи. При этом исследованию подлежат следующие вопросы: определение числа уровней подчинения; согласование целей между уровнями; распределение ответственности; выбор схем управления и контуров принятия решения; организация информационных потоков; выбор технических средств; оптимизация алгоритмов принятия решений.

При выборе технических средств связи и автоматизации определяющим входным фактором является информационный поток, подлежащий своевременной передаче. При обосновании исходных данных, уяснении требований Заказчика формулируется физическая и математическая постановка задачи на синтез структуры системы управления(связи) с учетом принятых ограничений, а по видуусловий функции определяется класс задачии метод её решения. Синтез перспективнойструктуры системы возможен и при снятии ограничений на параметры комплексов связи и автоматизации. В этом случае по результатам решения задачи синтеза можно обосновать требования к параметрам технических средств автоматизированных систем.

Решение задачи синтеза структур систем управления, связи с ограничениями на ресурс и без них позволяет определить гипотетическую систему управления (связи), оценить степень близости (по реализуемой эффективности) её и существующей системы и, на этой основе, обосновать:

– программу развития (совершенствования) существующей структуры;
– техническую политику в области связи и автоматизации.

При наличии сценариев функционирования систем, модели воздействия на систему управления и связи, представляется возможным разработать модель противоборства системы управления (связи) и системы воздействия, определить «стационарную точку» состояний противоборствующих систем и, на этой основе, определить типаж и количество необходимых

технических средств связи и автоматизации, что является основой для обоснования организационной структуры системы управления.

Если организационные мероприятия проведены, а техническая основа автоматизированной системы управления осталась прежней, то необходимо:

– разработать профильные модели должностных лиц для новых условий;

– разработать сетевую модель решения информационно-расчетных задач с учетом ихагрегирования «снизу-вверх»;

– провести тестирование организационной структуры «нового облика» с помощью матричных информационных моделей и перераспределить решаемые задачи.

Если окажется, что существующая техническая основа автоматизированной системы не эффективна, то необходимо решать задачу синтеза структуры системы управления и связи при уточнённых исходных данных.

Коцыняк М.А., Лаута О.С., Корень М.Ю., Сабан М.Ю., Нечепуренко А.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

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

Принято считать, что эффективность системы защиты ИТКС определяется только эффективностью средств защиты, что неверно. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

– средства разграничения доступа к информации в автоматизированных системах (паролирование);

– средства защиты информации при передаче ее по каналам связи (межсетевые экраны, криптомаршрутизаторы);

– средства защиты от информационного воздействия программ-вирусов (антивирусные системы и системы обнаружения вторжений).

Это означает, что ни одно отдельно выбранное средство защиты информации не может защитить ИТКС от комплекса целенаправленных воздействий - компьютерных атак (КА), а простая комбинация разнообразных средств защиты приводит к снижению эффективности защиты в целом из-за конфликтности параметров разнородных средств защиты.Трудности определения оценок эффективности СЗИ связаны с несовершенством существующего нормативно-методического обеспечения информационной безопасности.

С целью решения указанной проблемы необходимо первоначально оценить эффективность каждого средства защиты ИТКС и разработать методику синтеза системы киберзащиты ИТКС.

В настоящее время разработана методика синтеза системы киберзащиты ИТКС и произведена оценка эффективности средств защиты при комплексном воздействии КА.

Для оценки эффективности средств защиты разработаны профильные модели процесса преодоления КА средств защиты и с помощью метода топологического преобразования стохастических сетей определено среднее время преодоления средств защиты каждой КА. На основании этих значений, как исходных данных, рассчитанавероятность предотвращения средствами защиты воздействия КА на ИТКС.

Используя полученные значения, как исходные данные, по разработанной методике обоснованы требования к средствам защиты и произведен синтез системы защиты ИТКС.

Анализ полученных результатов показал, что:

– средства защиты неэффективны при комплексном воздействии КА.

– средства защиты на элементах ИТКС должны размещаться комплексно. С целью снижения стоимости системы защиты все средства защиты должны быть универсальными, реализованнымипрограммно и установленными в элементы ИТКС еще на этапе их изготовления;

– для выполнения требований по защите ИТКС требуется увеличить частоту смены параметров средств защиты.

Кречин И.В., Бунин А.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИС

Комплексная система защиты информации должна строиться с учетом четырех уровней любой информационной системы (ИС), в т.ч. и геоинформационной системы:

1. Уровень прикладного программного обеспечения (ПО), отвечающий за взаимодействие с пользователем. Примером элементов ИС, работающих на этом уровне, можно назвать текстовый

редактор WinWord, редактор электронных таблиц Excel, почтовая программа Outlook, броузер Internet Explorer и т.д.

2. Уровень системы управления базами данных (СУБД), отвечающий за хранение и обработку данных информационной системы. Примером элементов ИС, работающих на этом уровне, можно назвать СУБД Oracle, MS SQL Server, Sybase и даже MS Access.

3. Уровень операционной системы (ОС), отвечающий за обслуживание СУБД и прикладного программного обеспечения. Примером элементов ИС, работающих на этом уровне, можно назвать ОС Microsoft Windows NT, Sun Solaris, Novell Netware.

4. Уровень сети, отвечающий за взаимодействие узлов информационной системы. Примером элементов ИС, работающих на этом уровне, можно назвать протоколы TCP/IP, IPS/SPX и SMB/NetBIOS.

Система защиты должна эффективно функционировать на всех этих уровнях. Иначе злоумышленник сможет реализовать ту или иную атаку на ресурсы ГИС. Например, для получения несанкционированного доступа к информации о координатах карт в базе данных ГИС злоумышленники могут попытаться реализовать одну из следующих возможностей:

1. Прочитать записи БД из MS Query, который позволяет получать доступ к записям многих СУБД при помощи механизма ODBC или SQL-запросов (уровень прикладного ПО).
2. Прочитать нужные данные средствами самой СУБД (уровень СУБД).
3. Прочитать файлы базы данных непосредственно на уровне операционной системы.
4. Отправить по сети пакеты со сформированными запросами на получение необходимых данных от СУБД или перехватить эти данные в процессе их передаче по каналам связи (уровень сети).

Для того, чтобы нельзя было реализовать ту или иную атаку, необходимо своевременно обнаружить и устранить уязвимости информационной системы. Причем на всех 4 уровнях. Помочь в этом могут средства анализа защищенности (security assessment systems) или сканеры безопасности (security scanners). Эти средства могут обнаружить и устранить тысячи уязвимостей на десятках и сотнях узлов, в т.ч. и удаленных на значительные расстояния.

Совокупность применения различных средств защиты на всех уровнях ГИС позволит построить эффективную и надежную систему обеспечения информационной безопасности геоинформационной системы. Такая система будет стоять на страже интересов и пользователей, и сотрудников компании-провайдера ГИС-услуг. Она позволит снизить, а во многих случаях и полностью предотвратить, возможный ущерб от атак на компоненты и ресурсы системы обработки картографической информации.

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

МОДЕЛЬ ИНТЕГРАЦИИ СХЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА РАЗЛИЧНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Механизмы разграничения доступа присущи практически всем существующим автоматизированным системам (АС), причем как правило, это - дискреционный, мандатный и ролевой способы доступа. В связи с тем, что при создании единого информационного пространства (ЕИП) будут объединяться большое количество АС, то можно сказать, что с большой долей вероятности в создаваемом ЕИП окажутся АС у которых политика безопасности будет основываться на одном конкретном способе доступа. При создании ЕИП естественно нас коснется вопрос о создании единой системы разграничения доступа. Что касается разграничения доступа АС с одинаковыми схемами разграничения доступа (СРД), то решение таких задач уже не раз были упомянуты в различных источниках. Что же касается объединения АС с разными системами разграничения доступа, при создании ЕИП, то в таком аспекте эта проблема еще не рассматривалась.

В связи с тем что построение единой схемы разграничения доступа при данных условиях довольно проблематично, предлагаем ввести некоторую избыточность для каждой из трех отдельных схем разграничения доступа.

Для дискреционного способа разграничения доступа:

– множество пользователей и множество объектов доступа имеют одинаковые метки- для мандатной схемы разграничения доступа;

– все пользователи и все объекты доступа имеют одну роль – для ролевой схемы разграничения доступа.

Для мандатного способа разграничения доступа:

– множество пользователей имеет доступ ко всем объектам доступа – для дискреционной схемы разграничения доступа;

– все пользователи и все объекты доступа имеют одну роль – для ролевой схемы разграничения доступа.

Для ролевого способа разграничения доступа:

– множество пользователей и множество объектов доступа имеют одинаковые метки – для дискреционной схемы разграничения доступа;

– множество пользователей имеет доступ ко всем объектам доступа – для дискреционной схемы разграничения доступа.

Предполагается, что в информационном обмене, в едином информационном пространстве, участвует большое количество автоматизированных систем, которые могут иметь три различные схемы разграничения доступа: мандатную, дискреционную и ролевую. Причем количество АС с той или иной схемой разграничения доступа не лимитировано.

Для решения данного вопроса предполагается разбить создание единой схемы разграничения доступа на несколько этапов. На первом этапе мы попробуем объединить дискреционную схему разграничения доступа и мандатную схему разграничения доступа.

Считаю, что данный подход обеспечит достаточно высокую устойчивость функционирования системы разграничения доступа при функционировании ЕИП.

Лазаро Зеферино, Грака Жозе Да Сильва, МитрофановМ.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В процессе формирования информационного общества происходит активная разработка и внедрение во все сферы человеческой деятельности ИКТ. Информация и информационные ресурсы становиться одними из решающих факторов развития личности, общества и государства. Широки возможности компьютеров и ИКТ позволяют автоматизировать процессы мониторинга и управления государственными, экономическими, социальными, оборонными и другими объектами и системами, получать, накапливать и обрабатывать и передавать информацию об этих процессах практически с любой скоростью, в любом количестве. Естественно, что все это позволяет утверждать, что информация играет сегодня решающую позитивную роль в развитии человечества.

Но история учит нас тому, что многие достижения научно-технической мысли использовались не только во благо людей. Вспомним достижения ядерной физики – создание атомной бомбы, химии – отравляющие газы и т.д. всегда находились силы и структуры и даже государства, которые стремились найти двойное назначение любому открытию и успеху в научной и научно-технической сфере.

С указанных позиций вполне естественным является стремление определенных субъектов к единоличному обладанию информационными ресурсами, средствами и технологиями и их использованию в целях удовлетворения собственных интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. Информация и ИКТ при этом начинают выступать в качестве определенных угроз интересам конкурентов. При этом в полной мере проявляется закономерность, характерная для извечной проблемы соотношения защиты и нападения, которая в конце XIXвека была названа «борьбой брони и снаряда». Применительно к обсуждаемой ситуации можно утверждать, что в современных условиях «информационный снаряд» побеждает (опережает) в своем развитии «информационную броню».

Первый заместитель начальника Генштаба Вооруженных сил РФ генерал-лейтенант Алексей Бурутин на форуме «Информационные решения для безопасности России», проходившем 31 января 2008 года, заявил, что «достижение победы в возможных будущих войнах и вооруженных конфликтах будет достигаться путем уничтожения управления государством и Вооруженными силами за счет информационных технологий».

В обозримом будущем достижение конечных целей войн и вооруженных конфликтов будет решаться не столько уничтожением войск и сил противника, сколько за счет подавления его государственного и военного управления, навигации и связи, воздействия на другие информационные объекты, от которых зависит стабильность управления государством. Кроме того, с помощью информации можно воздействовать на людей и их мировоззрение. Такого рода воздействие, ведется,как правило, по линии разрушения духовных ценностей, путем воздействия на индивидуальное, групповое и массовое сознание населения.

Любое суверенное государство, должно принимать действенные меры для отражения атак с применением информационного вооружения. Концепции информационных войн, как правило включают в себя следующие компоненты: разрушение систем связи противника; перехват сообщений; взлом компьютерных сетей; воздействие на общественное мнение путем распространения дезинформации.

Противостоять такому воздействию весьма сложно. В настоящее время развиваются следующие направления защиты:

– совершенствование нормативно-правовой базы;

– формирование специальных подразделений информационной обороны;

– обучение персонала;
– совершенствование технических средств защиты информации;
– повышение эффективности организационных мероприятий.

Лаута О.С., Баленко А.А., Лаута А.С., Лянгузов Д.А., Лукина О.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

КИБЕРУСТОЙЧИВОСТЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

В современной войне первоочередными объектами направленного противодействия и поражения стали не войска и оружие, а системы управления противника. Прогнозируемый характер воздействия противника на систему управления и информационно-телекоммуникационную сеть (ИТКС) как ее техническую основу обусловливает появление новых требований к показателям качества функционирования ИТКС.

Использование в ИТКС технологий, средств связи и программного обеспечения иностранного производства, интеграция ИТКС с сетью связи общего пользования (ССОП), а ССОП – с мировым информационным пространством предопределили смещение акцентов на достижение превосходства над противником на основе применения компьютерных атак (КА).

Результатом воздействия КА являются блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации, отказы, сбои в работе ИТКС ВН, а также компрометация передаваемой (получаемой) информации.

В этом случае, КА – один из основных факторов, определяющих устойчивость ИТКС. Прогнозируемый характер воздействия КА на ИТКС обуславливает появление четвертой составляющей устойчивости – киберустойчивостии совокупности качественно новых требований, которым должны соответствовать показатели устойчивости ИТКС. Под киберустойчивостью понимается способность ИТКС обеспечивать управление войсками, силами и оружием в условиях воздействия КА.

Для решения проблемы обеспечения киберустойчивости ИТКС необходимо решение следующих задач:

– разработать методику прогнозирования распределения КА по уровням эталонной модели взаимодействия открытых систем (ЭМВОС);

– разработать методику оценки киберустойчивости ИТКС, позволяющую оценивать параметры ИТКС и обосновывать требования к параметрам;

– разработать методику синтеза системы защиты ИТКС.

В настоящее время указанные методики разработаны.

Анализ полученных результатов показал, что:

– воздействие КА носит системный характер (комплексно), что требует разработки методики оценки киберустойчивости, которая бы учитывала взаимосвязь традиционных параметров устойчивости (коэффициента связности), вероятностно-временных характеристик комплексных КА и вероятности их воздействия.

– кибеустойчивость и традиционное понятие устойчивости находятся в противоречии. Это позволяет определить оптимальное количество маршрутов для передачи информации и отранжировать маршруты по родам связи и по оперативности управления.

– структура системы защиты, должна включать в себя 2 рубежа (слайд):

a) сетевой, на базе интегрированных аппаратно-программных средств, реализующих принципы криптографии, межсетевого экранирования, системы разграничения доступа и системы обнаружения вторжений;

b) протокольный.

Левоневский Д.К., Фаткиева Р.Р.
Россия, Санкт- Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ИЗМЕРЕНИЕ КРИТИЧЕСКИХ ХАРАКТЕРИСТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Оценки информационных потоков в протяжённых компьютерных сетях позволяет сформировать признаки вредоносных воздействий. Это особенно актуально в свете всё возрастающей роли сетей в жизни общества, актуализации киберпреступности и информационных войн.Но при решении задачи оценки информационных потоков возникает комплекс проблем, характеризующийся тремя основными направлениями:

1. Отбор статистической информации (какие характеристики информационных потоков измерять, с какой частотой).
2. Определение необходимой глубины и масштабности сбора информации.

3. Формирование таких систем сбора и обработки информации о сети, которые сделают минимальной дополнительную нагрузку на информационно-вычислительную сеть и не воспрепятствуют её бесперебойному функционированию.

Существующие методы оценки трафика слабо учитывают влияние этих проблем. Возникают трудности масштабирования существующих методов. Кроме того, методы зачастую не поспевают за развитием аппаратных и программных средств. Это приводит к необходимости разработки новых моделей, методов и технологий комплексной оценки и прогнозирования сетевой безопасности, которые позволят получать глобальные оценки событий, осуществлять прогноз поведения и управление информационно-вычислительными системами.

В ходе решения этих задач получены следующие результаты:

1. Проведена систематизация и структуризация известных методов с привязкой к основным компонентам сетей;
2. Определены показатели сетевой безопасности как отдельных узлов и каналов, так и систем в целом;
3. Разработан ряд алгоритмов по комплексной оценке безопасности обнаружения атак;
4. Адаптирован ряд методов прогнозирования для решения задач оценки информационной безопасности;
5. Сформированы научно-практические рекомендации по оценке и прогнозированию информационной безопасности.

Все рекомендации разделены на 3 группы: к первой группе относятся рекомендации по построению перспективной распределённой системы комплексной оценки и прогнозирования сетевой безопасности, позволяющие повысить безопасность сиспользованием алгоритмов сбора и обработки данных о состоянии системы; ко второй группе относятся предложения, позволяющие оптимизировать процесс мониторинга сетевой безопасности с учётом ограничений по охвату и пропускной способности используемых каналов связи; к третьей группе относятся предложения по новым способам и средствам обеспечения сетевой безопасности компьютерных сетей.

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

МОДЕЛИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

Моделирование вообще, и математическое моделирование интеллектуальных (интеллектных) систем в частности, во многом определяют технологию нашего познания. Насколько адекватно мы моделируем действительность, настолько успешно мы её познаем. На основе адекватного познания мы и адекватно существуем в действительности. Мере адекватности можно сопоставить полноту учёта закономерностей рассматриваемой предметной области. Базовым законом является закон сохранения целостности объекта. Сущность этого закона определяется неразрывной связью объекта и его движения и характеризуется как взаимная трансформация свойств объекта и свойств его движения при заданном предназначении.Не учитывая на практике закон сохранения целостности объекта, мы сталкиваемся с тем, что результат применения созданной нами объекта не соответствует ожидаемому результату. Как раз при разработке новых систем управления этот закон в практике весьма часто не учитывается, что не позволяет адекватно реагировать как на сбои аппаратной части, так несанкционированные программные воздействия извне. В результате чего возникают различного рода затруднения в реализации потенциала их функционирования.

Как и все объекты окружающей действительности, рассматриваемые проблемно-ориентированные системы безопасности существуют в пространстве и времени и характеризуются пространственно-временными состояниями.

В докладе представлен подход моделирования безопасности в распределенных системах на множестве элементов распределенных в пространстве и времени, которые имеют два типовых противоположных по смыслу состояния на основе среды радикалов. В большинстве теоретических разработок, вопросы описания системы с двумя противоположными состояниями, опираются в основном на математической логике, которая, в свою очередь, не оперирует временем. Поэтому ее возможности страдают от концептуальной неполноты (описывает состояние системы без динамики) и не удовлетворяют рассматриваемому подходу, который определяет, что необходимо управлять на множестве распределенных элементов в пространстве и времени, которые имеют два противоположных состояния. Помимо этого, теория конечных автоматов позволяет описывать два состояния и их изменения во времени, но не содержит формализованного аппарата, который связывает конечные автоматы в пространстве и времени, то есть отсутствует механизм формирования поля.

В результате чего, анализ возможностей применения средств математической логики и теории конечных автоматов показывает, что задачи моделирования безопасностью в распределенной системе описываются на основе вербальной связи между элементами, что в неполной мере

позволяет автоматизировать процесс управления. Существующие подходы к моделированию интеллектуальных (интеллектных) систем, учитывающие аспекты пространства и времени, следует в большей мере увязывать с представлениями формально-аксиоматического метода, соответствующих механизмов реализации новых типов обратной связи.

Лепешкин О.М., Морозов М.М., Чернов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

РАЗРАБОТКА ФУНКЦИОНАЛЬНО-РОЛЕВОЙ МОДЕЛИ ДОТУПА

Анализ структурной модели коллективной задачи показал, что в них существуют отношения доступа двух видов. Первый вид отношений «клиент-сервер» характеризуется доступами к простым информационным объектам, а второй – «диалектически конфликтные пары ролей» - характеризуется доступами к сложным информационным объектам, где сложный информационный объект – это группа взаимосвязанных в соответствии с алгоритмом выполнения задачи простых информационных объектов. Наличие сложных информационных объектов приводит, с одной стороны, к появлению угроз доступа пользователей к неполной информации, а с другой стороны – к угрозе избыточного доступа при выполнении нескольких задач одновременно, и, таким образом, к угрозе нарушения целостности информации.

Это позволило сформулировать противоречия в теории и практике. Противоречия в практике возникают между системой безопасности и системой управления и выражаются в отсутствии механизмов динамического управления доступом, зависящего от текущего состояния системы и роли пользователя в ней. Противоречия в теории возникают между статическими моделями безопасности и динамическими моделями коллективных информационных задач.

Актуальность исследования определяется возрастанием сложности управления информационными процессами в социотехнических информационных системах, основой функционирования которых является обеспечение взаимодействия групп пользователей из распределенных социальных подсистем через общую информационную подсистему.

Появление таких коллективных информационных задач приводит к необходимости обеспечения функциональной безопасности как способности системы выполнять свои функции и задачи с заданными требованиями и ограничениями, где требования – выполнение коллективных задач, а ограничения – управление доступом в области информационной безопасности. При системе управления без функционально-ролевого разграничения доступа видно, что пользователями нарушается порядок выполнения коллективных задач, это определяется наложением процессов выполнения во времени и возможности невыполнения поставленных задач, а при введении функционально-ролевого управления доступом коэффициент ресурсной координации показывает уменьшение наложений, что означает верный порядок выполнения коллективных задач.

В нашей работе предложены принципы однозначного отображения методов структурного и функционального моделирования на среду радикалов.

Для активации схем радикалов функционально-ролевой политики безопасности предложено создание отчетов о функциональной безопасности выполнения коллективных информационных задач.

Предложена нами комбинация существующих статичных моделей ролевого и задачного разграничения доступа через динамические отношения коллективных задач, входящих и исходящих информационных потоков для задания условий выполнения коллективных задач и смены состояний пользователей.

Динамические отношения предложено осуществлять на основе среды радикалов для обеспечения безопасности коллективных задач. Смена состояний осуществляется через два вида полномочий: активные и полномочия перехода.

Логинов А.А., Кораблин В.О.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»

УНИФИКАЦИЯ СРЕДСТВ СБОРА ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИЙ

С развитием телекоммуникаций неизбежно увеличивается спектр возможных угроз и уязвимостей. Использование новых типов устройств, новых протоколов связи, количественное приращение элементов телекоммуникационной сети создает большое количество новых угроз, а, как следствие — событий безопасности. Без получения полной и достоверной информации о событиях безопасности невозможно построить систему защиты, однако множество разнородных источников данных событийного мониторинга порождает проблему сбора информации, основанную на разных протоколах функционирования, форматах данных, типах событий и т.д.

Решением данной проблемы могут служить унифицированные системы сбора данных, основанные на динамически подгружаемых программных модулях, метауправлении и гибкой

конфигурации. Такая система способна обеспечить сбор, обработку полученных данных по заданным правилам и передачу итоговых (обработанных) данных заданному получателю. Реализация взаимодействия с конкретным источником данных посредством введения программных модулей позволяет без изменений основной части системы оперативно вносить новые типы источников данных. За счет наличия встроенной категоризации получаемых данных по типу источника на основе использования модулей сбора данных упрощается обработка данных событийного мониторинга, а обработка основной частью системы, например, категоризация по типу событий, значительно облегчает последующий анализ событий безопасности.

Динамически подгружаемые программные модули просты в разработке и в применении, их использование позволяет обеспечить конфигурирование системы сбора данных под конкретную ситуацию, связанную с изменением количества типов источников данных. Такие модули создаются для семейств моделей телекоммуникационного оборудования, операционных систем и иных аппаратных и программных источников данных.

Метауправление, обеспечивающее задание параметров, подлежащих сбору с источников данных, позволяет оптимизировать работу с данными за счет работы только с необходимым и достаточным минимумом параметров. Это упрощает передачу данных по сетям телекоммуникаций, ускоряет анализ, предотвращает избыточность данных.

Конфигурирование средств сбора данных обеспечивает тонкую настройку системы под конкретную телекоммуникационную сеть посредством изменения файлов конфигурации. Так же можно обеспечить предварительную обработку и пересчет значений параметров для упрощения оперативного контроля. Например, получая значение параметра, определять, лежит ли она в определенном диапазоне и передавать уже логическое значение. Такие задания на пересчет могут задаваться посредством конфигурации.

Построенные на описанных принципах средства сбора данных позволяют обеспечить быструю адаптацию, простую настройку, оперативное функционирование.

Молдовян А.А., Ковцур М.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича

ОЦЕНКА СКОРОСТНЫХ ХАРАКТЕРИСТИК РЕАЛИЗАЦИИ АТАКИ ТИПА ПЕРЕБОР ПАРОЛЯ НА IP-АТС ПРИ ИСПОЛЬЗОВАНИИ FAIL2BAN

При организации корпоративной IP-телефонии может возникнуть задача предоставления доступа мобильным пользователям к ресурсам IP-АТС из сетей общего пользования. Таким образом, нелегитимные пользователи наравне с легитимными смогут выполнять авторизацию на IP-АТС, что позволит нарушителю реализовать атаку перебор пароля для захвата ресурсов IP-АТС.

Для защиты АТС от данной атаки распространено использования инструмента Fail2BAN. Однако, отсутствуют обоснования по выбору значений параметров для этого приложения. Целью данной работы является формирование рекомендаций по выбору значений параметров этого приложения, а также оценка скорости реализации атаки перебора пароля при использовании Fail2Ban.

Для регистрации на телефонной станции VoIP-клиент использует процедуру, представленную в RFC3261. Нелегитимный пользователь может воспользоваться процедурой регистрации для перебора пароля. Тогда определяющими для оценки временных характеристик атаки перебора будет как длина пароля и размер используемого алфавита, так и максимальная скорость, с которой нарушитель будет выполнять атаку. Скорость перебора пароля со стороны злоумышленника будет ограничена значениями максимальной допустимой скорости передачи и приема канала связи согласно тарифному плану владельца, максимально возможным числом регистраций в секунду, обеспечиваемым IP-АТС и зависящим от используемого программного и аппаратного обеспечения, максимально допустимым числом регистраций с учетом ограничений приложения Fail2ban, а также возможностями перебора пароля со стороны активного нарушителя.

Одним из инструментов, используемых для защиты от атаки перебора пароля, является приложение Fail2Ban.

Пользователь настраивает параметры приложения и активирует защиту.В этом случае, если хост выполняет несколько неуспешных попыток авторизации, превышая установленный порог, нарушитель блокируется приложением на некоторое время средствами LinuxIptables.

Правила блокировки создаются автоматически средствами Fail2Ban и удаляются через установленное время.Исследование показало, что выбор опций Fail2Ban необходимо осуществлять, основываясь не только на производительности IP-АТС, но и на скорости имеющегося канала связи. Составлена аналитическая зависимость времени блокировки хоста от порогового значения числа неуспешных авторизаций, числа хостов, находящихся под управлением нарушителя, а также производительности IP-АТС.

Молтянинов А.К., Москаленко К.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБОСНОВАНИЕ ПО РЕАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ МНОГОАГЕНТНОЙ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЯМИ СВЯЗИ

Реализация стратегий автоматизации процессов управления связью, заключается в разработке и внедрении эффективных информационных технологий, обеспечивающих в реальном масштабе времени замкнутость циклов организационного (оперативного) и технологического управления связью, существенно повышающих обоснованность и согласованность принимаемых решений должностными лицами по связи.

Одной из причин недостаточного уровня эффективности функционирования сетей связи заключается в том, что для них принята система управления, в которой принятие решений осуществляется на основе показателей работоспособности элементов сети или отдельных направлений связи, а также анализа сетевых ресурсов. При этом данная система управления является реактивной, а не проактивной, в соответствии с чем, она включается в процесс управления в тот момент, когда событие требующее реакции системы управления уже произошло.

Основным недостатком такого подхода является субъективность принятия решения в практическом большинстве случаев. Данное положение связано с тем, что в неполном объёме определены аналитические зависимости между состоянием конкретных сетевых элементов и соответствующих сетевых ресурсов и потребительскими характеристиками сети. То есть, существующую модель сетевого управления невозможно использовать для прогнозирования поведения сетевых элементов при их функционировании в составе сети, что является основным недостатком системы управления сетями связи.

Обеспечение способности сетей связи к самоорганизации, а также адаптации ее элементов к различным условиям функционирования требует разработки новых методов управления с привлечением технологий обработки знаний путем интеграции традиционных подходов и методов математического моделирования с применением моделей искусственного интеллекта, что позволяет построить интеллектуальную систему управления связью.

В основу построения такой системы управления сетями связи целесообразно положить современные технологии интеллектуальной многоагентной системы обработки управленческой информации, которые позволяют перейти от предположений, справедливых только для изолированных систем искусственного интеллекта, от индивидуальных систем, к распределённой обработке информации, ориентированной на данные и знания, сосредоточенные как в едином информационном хранилище, так и в различных взаимодействующих источниках. При этом организация программной среды должна базироваться на принципах создания распределённых многоагентных систем (или систем параллельных и распределённых «интеллектуальных агентов» и взаимодействующих источников данных и знаний). Процесс управления рассматривается в виде единой конструктивно развивающейся формальной системы, потока работ по автоматизированному управлению, который выполняется коллективом должностных лиц управления – так называемых агентов-управленцев и программно-аппаратных агентов интеллектуальной системы управления.

Москаленко К.Н., Молтянинов А.К.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОБОСНОВАНИЕ ПРОБЛЕМЫ ПО УПРАВЛЕНИЮ СЛОЖНЫМИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

В процессе управления сложными организационно техническими объектами целесообразно использовать обмен речевыми командами или сообщениями между должностными лицами. В ходе организации управления системами на больших расстояниях при чрезвычайных ситуациях используются низкоскоростные радиоканалы, образованные КВ и УКВ радиосредствами. При этом спектр услуг должностным лицам необходимо расширять, данное требование возможно реализовать в полном объеме при наличии высокоскоростных каналов связи. Тем самым возникает противоречие между потребностями и реальными возможностями радиосредств.

Одним из путей решения данной проблемы является уменьшение доли речевого трафика в общем объеме. Основными направлениями устранения избыточности речевых сообщений при их передаче является линейная и нелинейная фильтрация и последующее кодирование речевого сигнала.

Для анализа возможности максимального устранения избыточности речевого сигнала в работе предполагается рассмотреть функцию перехода через нулевые значения временной характеристики речевого сигнала. Последующее кодирование моментов перехода через нулевые значения позволит представить речевой сигнал в цифровой форме и использовать известные методы шифрования данных. Таким образом, это позволит решить следующие задачи:

1. Расширение спектра услуг, предоставленных должностным лицам для управлениясложными организационно-техническими объектами при чрезвычайных ситуациях.

2. Обеспечение безопасности передаваемой информации между должностными лицами.

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

МЕТОД КОМПЛЕКСНОЙ ОБРАБОТКИ ИНФОРМАЦИИ В АППАРАТУРЕ ПЕРЕДАЧИ ДАННЫХ

Устойчивость системы связи – способность системы связи обеспечивать управление войсками в условиях воздействия на ее элементы различных видов оружия противника, опасных факторов техногенного и природного характера и всех видов помех.

Рассматривая АПД как элемент системы связи, необходимо обеспечить выполнение главной возложенной на нее функции, а именно, передача сообщений в условиях помех.

Анализ алгоритмов обработки информации на примере современной АПД ПД-401 показал, что предлагаемые методы обработки информации, основанные на принципах циклического кодирования и применение решающей обратной связи для обеспечения ее достоверности не обеспечивают защиту от навязывания ложной информации.

Устранить данный недостаток возможно путем разработки метода комплексной обработки информации в АПД, обладающего следующими свойствами:

– согласованность по входным и выходным данным с существующей АПД;
– минимальная вероятность необнаруженной ошибки в канале связи;
– обнаружение и идентификация имитационных помех.

Решение поставленной задачи предлагается путем согласованного применения различных кодов с выделением и использованием их положительных свойств.

Предложенный метод представлен совокупностью способов (алгоритмов) обработки информации, позволяющих обеспечить:

– перестановка символов – преобразование пакета ошибок в одиночные независимые ошибки;
– имитостойкое кодирование – исправление одиночных ошибок, а также обнаружение и идентификация имитационных помех;
– циклическое кодирование – контроль необнаруженных ошибок.

Новизна предложенного метода обработки информации, с возложением новых свойств на аппаратуру передачи данных, заключается от известных новой совокупностью и последовательностью применения согласованных алгоритмов, направленных на пошаговую декомпозицию помех с идентификацией имитационных помех, с целью уменьшения вероятности навязывания ложной информации и вероятности необнаруженной ошибки. Основным элементом предлагаемого метода обработки информации является способ имитостойкого сверточного кодирования, основанный на совместном применении криптографического преобразования и помехоустойчивого кодирования в рамках единого алгоритма при однократном введении избыточности, что обеспечивает обнаружение имитационных воздействий противника в АПД на уровне исправления ошибок канала связи.

Новым техническим решением устройства имитостойкого сверточного кодирования является совмещение функций кодера канала с функциями узла наложения шифра в одном устройстве, в результате чего обеспечивается:

– помехоустойчивое сверточное кодирование, обеспечивающее обнаружение и исправление ошибок;
– отображение по определенному правилу соответствия сообщения в конкретный сигнал, принадлежащий множеству кодовых комбинаций сигналов, применяемых в системе (тем самым достигается имитостойкость, так как преобразование осуществляется с использованием закрытого ключа).

Олимпиев А.А.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

АТРИБУТНАЯ И РОЛЕВАЯ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА К ОБЪЕКТНОЙ МОДЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Выполнение процедур, направленных на удовлетворение растущих потребностей населения в связи, приводит к интенсивному и экстенсивному развитию телекоммуникационных сетей, в том числе обеспечению их надежного функционирования. В результате практически ни одна современная телекоммуникационная сеть не обходится без достаточно мощного комплекса средств планирования, контроля и управления — автоматизированной системы управления связью (АСУС).

На сегодняшний день в основу почти любого программного обеспечения, предназначенного для организации управления связью, положены информационные и математические модели телекоммуникаций, представленные в форме объектной модели, что обусловлено широким

распространением автоматизированных системам проектирования и языков программирования, использующих объектно-ориентированного подход (ООП).

Основные методы ООП при моделировании телекоммуникаций следующие:

– любая сущность телекоммуникационной сети представляется в форме объекта;

– каждый объект характеризуется набором параметров, представленных в форме атрибутов объекта, и набором функций чтения/записи над атрибутами, представленных в форме методов;

– над объектами определяется отношение общности, позволяющее разбить их на классы;

– взаимодействия объектов, существующие в телекоммуникационной сети, и их отношения формализуется в связях, представленных в форме атрибутов объектов или классов (в некоторых случаях взаимодействия и отношения могут быть представлены как самостоятельный объект);

– множество связей делится на однотипные группы, отражающие отдельные аспекты, плоскости, фрагменты и профили телекоммуникаций как объекты.

Международные рекомендации по построению АСУС предполагают существование пользователей, обладающих разным уровнем доступа к информации о телекоммуникациях, что обусловливает необходимость исследования видов деятельности этих пользователей и разработки базовых моделей доступа к информации при проектировании программного обеспечения АСУС. В основу этих моделей предлагается положить атрибутную модель разграничения доступа, которая в сравнении с ролевой моделью имеет достаточно удобный механизм формирования правил, позволяющий не только отобразить организационную структуру предприятия на иерархию ролей, но и поставить правила разграничения доступа в соответствие видам деятельности предприятия связи.

Традиционно при разработке моделей разграничения доступа, выделяют несколько наиболее общих видов деятельности предприятия связи, например: администрирование, мониторинг и управление связью, планирование и т.п.; и группы пользователей (субъектов управления), выполняющих определенные бизнес-роли. Каждому виду деятельности ставится в соответствие набор операций, задач и объектов, по отношению к которым субъектам приписываются полномочия. При достаточно большом количестве видов деятельности и субъектов возникает необходимость, чтобы одна и та же информация предоставлялась в разных формах и редактировалась разными способами, в результате чего ролевая модель перестает справляться с формированием единого пространства полномочий, учитывающего все возможные ситуации, в то время как правило, базирующееся на применении атрибутной модели, может быть представлено достаточно простым логическим выражением, связывающим атрибуты субъекта, объекта, вид деятельности и время.

Применительно к объектной модели телекоммуникационной сети одномерная модель доступа, где субъекту назначаются полномочия на определенную функцию управления конкретным объектом, превращается в многомерную модель, в которой субъектам, относящимся к разным профилям управления (безопасностью, функционированием, планированием) могут быть доступны одни и те же операции, но выполняемые в контексте разных задач. При этом в рамках одного профиля субъекту может быть доступен объект на управление на разных уровнях (сетевом, прикладном, канальном), в результате чего у субъекта управления могут оказаться разные полномочия на выполнение одной и той же функции в разные моменты его работы, что практически может быть описано достаточно простым логическим выражением, связывающим атрибуты объекта и атрибуты субъекта.

Примером может служить ситуация, когда инженер по безопасности предприятия может управлять портами устройства только в рамках задачи предотвращения несанкционированного доступа. С описанием такого правила атрибутная модель разграничения доступа справляется достаточно легко, а в ролевой модели в такой же ситуации используется механизм оперативного (динамического) переключения ролей или изменения полномочий, что увеличивает риски предприятия связи, так как роль, которую использует субъект для работы, он выбирает самостоятельно.

Павленко Е.Ю., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ДЕЦЕНТРАЛИЗОВАННЫХ СЕТЕЙ НА ОСНОВЕ АНАЛИЗА ПОТОКОВ ПЕРЕДАЧИ СЕТЕВОГО ТРАФИКА

В настоящее время обеспечение анонимности клиента в сети Интернет становится важной и актуальной темой. Безопасность данных при работе в глобальной сети сегодня не ограничивается только защитой пользователя от вирусов или мошенников. Фактически, любое действие — просмотр и загрузка контента, оставление комментария, переход на веб-страницу — может использоваться в коммерческих целях для рассылки спама или формирования целевой рекламы, а также злоумышленниками для проведения целенаправленных атак (APT-атак).

Впервые анонимные системы связи были представлены в основополагающей работе Дэвида Чаума в 1981. Суть работы заключается в том, что анонимность достигается путем пересылки сообщений через серию передаточных узлов, называемых микс-узлами (перемешивающие узлы).

Каждый микс-узел выполняет две основные задачи. Первая — это обеспечить побитовую неразличимость сообщений, вторая — перемешать поток сообщений.

Чтобы на выходе из узла нарушитель не смог идентифицировать отслеживаемое сообщение по его содержимому, все входящие сообщения приводятся к одному размеру (короткие сообщения дополняются случайными данными) и шифруются. Это и есть обеспечение побитовой неразличимости.

Перемешивание потока сообщений используется для того, чтобы нападающий не мог сопоставить время входа сообщения в узел со временем его выхода, и, таким образом, понять, какое именно исходящее сообщение соответствует искомому. Узел некоторое время накапливает входящие сообщения, перемешивает их и отправляет дальше в случайном порядке.

Сеть анонимизации TOR (TheOnionRouter) — это система анонимной связи с малыми задержками, в основе которой лежат цепочки передаточных узлов. Это улучшенная версия так называемой «луковичной маршрутизации» OnionRouting. OnionRouting (OR) — это технология анонимного обмена информацией через компьютерную сеть, основанная на использовании многослойного шифрования. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторится. Таким образом, промежуточные узлы не знают источник, пункт назначения и содержание сообщения.

В результате исследования алгоритмов работы и архитектуры сети анонимизации TOR были выявлены следующие особенности, который могут быть использованы злоумышленниками для проведения атак статистического анализа трафика:

В сети TOR выходной узел цепочки анонимизации передает трафик пользователя в открытом виде, что создает возможность нарушителю обрабатывать трафик пользователя в открытом виде.

Первый узел цепочки анонимизации знает реальный IP-адрес пользователя, т.е. в случае определения того, что именно этот узел является первым для того или иного пользователя, можно однозначно его деанонимизировать.

Сеть TOR не защищена от возможности создания паттернов трафика на узлах сети, которые могут быть использованы для оценки корреляции таких паттернов на разных узлах, что позволит выявить узлы, образующие цепочку анонимизации.

В работе проведена оценка вероятности контроля злоумышленником входного и выходного узлов цепочки анонимизации в сети TOR, которая показала, что если злоумышленник контролирует 1000 входных и 500 выходных узлов, он с вероятностью 25% сможет контролировать нужное соединение. Стоит отметить, что реальная вероятность контроля соединения меньше, т.к. не все входные узлы сети TOR являются публичными, в виду того, что в некоторых странах ведется активная борьба с сетью TOR и открытые IP-адреса входных узлов заблокированы.

Для корректировки данной оценки было разработано специальное программное обеспечение, которое осуществляет сбор статистических параметров трафика с узлов сети анонимизации TOR и осуществляет построение графика распределения сетевого трафика по узлам сети.

В результате работы рассмотрены особенности функционирования сети анонимизации TOR, исследованы существующие атаки, направленные на деанонимизацию пользователей, выполнены теоретическая и экспериментальная оценки проведения деанонимизации на основе создания паттернов сетевого трафика, а также разработано специальное программное обеспечение, осуществляющее сбор и анализ статистических параметров, полученных от узлов сети TOR.

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

ПРОБЛЕМЫ БОЛЬШИХ ДАННЫХ. ОСОБЕННОСТИ И ПУТИ РЕШЕНИЯ

В настоящее время крайне актуальной становится проблема взрывного роста объема накапливаемых данных и неспособности современных аналитических, технических и программных средств справиться с ней.

В докладе обсуждаются источники Больших Данных, свойства, структура и классификация Больших Данных.Важное внимание уделено истории проблемы, сущности современных понятий «Большие Данные», «аналитика Больших Данных», «информация», «данные», «наука о данных».

Рассматриваются подходы и методы преодоления данной проблемы. Отмечается, что владеть данными намного сложнее, чем владеть материальными активами, большие массивы данных сложно обрабатывать, данные довольно просто тиражируются и вероятность их хищения гораздо выше, чем кражи материальных предметов.

В докладе подробно рассматриваются существующие программные и аппаратные средства для работы с Большими Данными и исследуются их реальные возможности.

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

ПОКАЗАТЕЛИ ДОСТУПНОСТИ ЛЕГАЛЬНЫХ (АВТОРИЗИРОВАННЫХ)ПОЛЬЗОВАТЕЛЕЙ К ЗАЩИЩАЕМОМУ ИНФОРМАЦИОННОМУ РЕСУРСУ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Вектор показателей доступности легальных (авторизированных) пользователей телекоммуникационных сетей (ТКС) к защищаемому информационному ресурсу включает показатели временной доступности – своевременности и топологической доступности, призванные количественно описывать способность (свойство) процесса защиты информации (ЗИ):предоставлять пользователям ТКС услуги безопасного доступа к защищенной информации тогда, когда это им необходимо, в необходимом пользователям услуг месте и в течение требуемого времени (продолжительность предоставления услуг) с требуемым качеством (достоверность и целостность предоставления услуг).

Вектор показателей доступности легальных (авторизированных) пользователей ТКС к защищаемому информационному ресурсу имеет две составляющие – временную (когда, своевременность) и топологическую (где). В качестве одного из основных свойств процесса ЗИ выступает временная доступность или своевременность, рассматриваемая как способность процесса ЗИ обеспечивать доступ пользователей ТКС к защищаемым ресурсам сети и предоставление им требуемого перечня безопасных услуг в установленные сроки. Показатель своевременности доступа пользователей ТКС к защищаемым ресурсам сети может быть выражен через время ожидания доступа к конкретной услуге, а с учетом многообразия угроз безопасности информации для каждого конкретного из множества сервисов (услуг), реализуемых и предоставляемых пользователям, своевременность доступа легальных (авторизированных) пользователей сети к защищаемому информационному ресурсу можно охарактеризовать интегральным (по всему перечню услуг и соответствующих им угроз) показателем –средним временем доступа пользователей ТКС к защищаемому информационному ресурсу.

Кроме того, временная доступность легальных (авторизированных) пользователей может количественно характеризоваться интенсивностью отказов в доступе, вызванных сбоями (ошибками) при реализации процесса ЗИ, а также средним временем межу отказами в доступе.

Помимо обеспечения услугами за необходимое время, легальным(авторизированным) пользователям ТКС должна быть обеспечена топологическая доступность к защищаемому информационному ресурсу, т.е. доступ к защищенным услугам в необходимом им месте. Иными словами, должны соблюдаться требования по топологической доступности к защищаемой информации, причем как для пользователей ТКС, построенных на основе кабелей, так и для пользователей беспроводных ТКС. В этом случае топологическая доступность зависит от радиуса контролируемой зоны, от радиуса зоны охвата точки доступа беспроводных ТКС, от удаленности пользователя и от параметров радиосигнала.

Таким образом, показатели доступности, составляющие содержание вектора показателей топологической доступности, количественно характеризуют способность процесса ЗИ не препятствовать доступу легальных (авторизированных) пользователей ТКС к защищаемому информационному ресурсу и не затруднять предоставление им требуемого перечня услуг ТКС в установленном месте их нахождения и при перемещении пользователя. В итоге, векторный показатель доступности легальных (авторизированных) пользователей ТКС к защищаемому информационному ресурсу, характеризует свойство процесса ЗИ обеспечивать пользователей ТКС услугами безопасного доступа к защищенной информации тогда, когда это им необходимо и там, где это необходимо.

Паращук И.Б., Порецков О.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПАРАМЕТРЫ ЦЕЛОСТНОСТИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Известно, что вектор параметров целостности информации при реализации процесса защиты информации (ЗИ), циркулирующей в телекоммуникационной сети (ТКС), должен содержать параметры, численно характеризующие точность, достоверность и полноту защищаемой информации, а также защищенность хранимой, обрабатываемой, передаваемой и принимаемой информации от возможных непреднамеренных и злоумышленных искажений.

Иными словами, это свойство процесса ЗИ обеспечивать без чрезмерного ухудшения, с соблюдением требований (границ) по безошибочности и по точности (достоверности) и неискаженности хранимой, обрабатываемой, передаваемой и принимаемой информации, т.е. с соблюдением требований по числу ошибок и искажений информации.

Таким образом, целостность информации при реализации процесса ЗИ в ТКС должна включать два компонента – достоверность (точность, безошибочность) и неискаженность (отсутствие искажений) в процессе ЗИ при ее хранении, обработке, передаче и приеме в ТКС.

Целостность с точки зрения сохранения достоверности и точности информации при реализации процесса ЗИ, может оцениваться коэффициентом потери достоверности информации, хранимой, обрабатываемой, передаваемой и принимаемой в рамках ТКС.

Этот коэффициент, с учетом мультисервисной информации, хранимой, обрабатываемой, передаваемой и принимаемой в рамках сети, включает потери слоговой разборчивости в виде количества утерянных (непонятых, искаженных до неузнаваемости) слов и словосочетаний для IP-телефонии, количество неправильно опознанных образов при реализации в рамках ТКС видеоконференцсвязи, а также количество ошибочно (искаженно) принятых, обработанных, хранимых и переданных данных при реализации услуг в рамках сетей, ориентированных на передачу данных.

В общем случае, учитывая многообразие угроз безопасности информации для каждого конкретного из множества сервисов (услуг), реализуемых и предоставляемых пользователям в рамках ТКС, интегральный коэффициент потери достоверности информации можно сформулировать с учетом относительной опасности (сложности преодоления) конкретной угрозы при предоставлении конкретной услуги, в зависимости от вида услуги, подлежащей защите, а также с учетом вероятности достоверной передачи при функционировании системы ЗИ в условиях воздействия угроз.

С учетом того, что параметр неискаженности (отсутствия искажений) информации при реализации процесса ЗИ численно характеризует способность процесса ЗИ реализовать противодействие модификации или разрушению информации, хранимой, обрабатываемой, передаваемой и принимаемой в ТКС, он может быть представлен в виде коэффициента искажений (пакетов, блоков данных и т.п.). Физический смысл данного коэффициента – отношение количества искаженных данных к общему числу хранимых, обрабатываемых, передаваемых и принимаемых по сети данных. При этом, данный коэффициент должен быть минимальным, стремиться к нулю.

Пицун А.Л., Байбиков Г.Р.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ И ПУТИ ИХ РЕШЕНИЯ

В связи с развитием информационных технологий в системах специального назначения возросла проблема защиты информации от несанкционированного доступа.

Авторами рассматривается вопрос обеспечения защиты информации от несанкционированного доступа на защищенных объектах военного назначения.

Основными проблемами защиты информации от НСД в системахВН является:

– проблема защиты информации от внутренних угроз;

– проблема защиты программных и технических средств автоматизации от вредоносного кода, аппаратных и программных закладок, компьютерных атак;

– проблема защиты информации, передаваемой по арендуемым каналам и сетям передачи данных;

– проблема защиты информации в условиях информационной (компьютерной) войны, характеризующихся массовой реализацией неизвестных ранее угроз, в том числе и компьютерных атак;

– проблема организации комплексной защиты на объектах автоматизации военного назначения;

– переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

– объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

– увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Традиционно для организации доступа к информации использовались организационные меры, основанные на строгом соблюдении должностными лицами процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами. Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации в системах специального назначения.

Это связанно с тем, что количество угроз безопасности информации постоянно возрастает. В первую очередь следует отметить расширение каналов утечки информации за счет несанкционированного доступа, что определяет необходимость проведения постоянного анализа и модернизации существующих средств защиты.

Репников А.Ю., Худайназаров Ю.К., Штаненко В.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

КОНТРОЛЬ В ПРОБЛЕМАТИКЕ ЗАЩИТЫ СИСТЕМЫ СВЯЗИ ОТ РАДИОРАЗВЕДКИ

Проблемы разведзащищенности современной системы связи обусловлены, как высокими оперативно-техническими возможностями современных средств технической разведки, так и ограниченными возможностями системы связи существующих типов по защите от них (защитным потенциалом). Так, например, современные системы радиоразведки, способны обнаруживать работу источников радиоизлучений в диапазонах частот до 25 – 25 ГГц и расстояний 300 – 500 км (в т.ч. и сигналов от искусственных спутников Земли), если выходные (эффективные) мощности радиопередатчиков превышают несколько десятков ватт.

Основные проблемы защиты существующих линий связи от радиоразведки обусловлены следующими факторами:

– жестким закреплением выделенных для военных радиолиний частотных диапазонов и их дополнительным перераспределением (уже в рамках военного ведомства) под вполне определенные типы радиосредств (радиорелейные, тропосферные, спутниковые и пр.);

– значительным числом разведпризнаков, содержащихся в излучаемых радиосигналах (по видам модуляции, к числу каналов связи, стабильности несущих частот и пр.);

– преимущественным использованием в отечественной военной связи частотных диапазонов, электромагнитно доступных для современных средств радиоразведки (F ≤ 10…20 ГГц);

– значительными мощностями радиоизлучений радиостанций. Например, типовые значения эффективной мощности передатчиков (Рпрд. эф. = Рпрд × Ga, где Ga – коэффициент усиления антенны), состоящих на вооружении радиостанций, находятся в следующих в следующих пределах: $10^2 \ldots 10^4$ Вт для средств декаметровой) и метровой радиосвязи, до $10^4 \ldots 10^8$ Вт для средств тропосферной и спутниковой связи;

– широким использованием в линиях связи каналов связи (служебной связи), переговоры по которым ведутся исключительно в открытом режиме. В рамках всех видов разведки последнему фактору принадлежит особая роль, поскольку позволяет противостоящей стороне по содержанию ведущихся переговоров оценивать эффективность применения средств противодействия военной связи.

Системный подход к обеспечению безопасности связи предполагает разработку и реализацию мероприятий защиты от всех видов разведки на всех этапах функционирования системы связи. Процессуправления безопасностью связи должен включать этап оценки эффективности защитных мер, который реализуется соответствующей подсистемой.

Действующая концепция тотального семантического контроля безопасности связи (КБС) приводит к тому, что ее возможности должны стремиться к возможностям системы технической разведки. При этом должны выполняться требования своевременности, полноты и достоверности КБС.Широкое применение шифровальной аппаратуры связи приводит к тому, что семантика становится недоступнойдля радиоразведки, поэтому приоритетными становятся возможности технического анализа и выявления оперативно-тактических признаков объектов разведки.

В связи с этим актуальными задачами совершенствования системы обеспечения безопасности связи являются:

1. Оптимальное распределение ресурсов подсистемы КБС;

2. Обеспечение взаимодействия с автоматизированной системой управления связью с целью достаточного информирования подсистемы КБС о состоянии и прогнозируемых изменениях системы связи;

3. Совершенствование методов и средств технического и оперативно-тактического анализа, а также развитие методологии оценки реальной разведзащищенности системы связи.

Рожнов М.Д., Мач Д.П., Шерстюк М.Ю.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

ФИЛЬТРАЦИЯ СОБЫТИЙ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одной из наиболее важных составных частей любого современного средства обеспечения информационной безопасности является система управления событиями информационной безопасности - система класса SecurityInformationManagement (SIM). SIM система должна заниматься классификацией событий информационной безопасности, их сбором, хранением, а также автоматическим анализом событий на предмет выявления инцидентов нарушения информационной безопасности.

Автоматический анализ событий информационной безопасности должен выполняться либо путем простой фильтрации событий на предмет выявления только самых значимых по заданным критериям отбора, либо путем выполнения сложных алгоритмов поиска инцидентов нарушения

информационной безопасности по специально созданным экспертами для этих целей шаблонам поиска.

В некоторых ситуациях весьма эффективным может быть ручной анализ событий мониторинга информационной безопасности на основе предоставления эксперту по безопасности отфильтрованных событий по определяемому экспертом правилу отбора событий. В этом случае эксперт может определить множество взаимосвязанных событий, являющихся в целом основанием полагать о возникновении инцидента нарушения информационной безопасности, что зачастую не может быть выявлено при автоматическом анализе событий т. к. либо отсутствует шаблон поиска для данного вида нарушений безопасности, либо правило поиска имеет настолько сложный и не очевидный характер, что зачастую написание алгоритма поиска подобных нарушений является довольно сложной и ресурсоёмкой задачей, в то время, как опытный эксперт по безопасности может справиться с этой задачей быстрее.

Как при автоматическом, так и при ручном анализе событий информационной безопасности, ключевую роль играет механизм отбора событий по некоторому правилу - фильтрация событий. В качестве механизма фильтрации событий информационной безопасности может выступать функция отбора событий по специальному логическому выражению фильтра, которое может вернуть Истину - в случае удовлетворения события логическому выражению фильтра, либо Ложь в случае, когда событие не удовлетворяет логическому выражению фильтра:

событие ИБ → [Фильтр] = Истина | Ложь

Логическое выражение фильтра должно учитывать структуру событий информационной безопасности - события должны отличаться друг от друга по набору заранее установленных характеристик, например: типы источников, категории важности, типы событий, временные метки регистрации средствами защиты информации и другие. Набор отличительных характеристик событий далее будем именовать атрибутами.

Логическое выражение фильтра должно позволять выполнять типовые операции сравнения над значениями атрибутов события: больше, меньше, равно, не равно, больше или равно, меньше или равно и вхождение в перечень значений.

Логическое выражение фильтра должно позволять выполнять типовые логические операции для комбинации нескольких операций сравнения в более сложное, такие, как: логическое отрицание, логическое «И», а также логическое «ИЛИ».

Логическое выражение фильтра должно позволять определять порядок выполнения логических операций посредством расстановки скобок, определяющих приоритет применения логических операций.

В качестве механизма формирования логического выражения фильтра отбора событий информационной безопасности может быть применён либо ручной ввод выражения фильтра в виде текста, либо графический ввод выражения фильтра с использованием общепринятых графических элементов управления.

В случае ручного ввода выражения фильтра требуется задание заранее определенными константами атрибутов событий, а также перечисляемых значений, которые имеют строго заданный ограниченный домен значений.

В случае графического ввода выражения фильтра конструктор выражения может быть визуально представлен в виде организационной структуры типа дерево, узлами которого являются логические операции «И» и «ИЛИ», к которым также может быть применена операция логического отрицания «НЕ». Листьями этого дерева могут выступать логические выражения, построенные на операциях сравнения и включения, а также вложенные логические операции И» и «ИЛИ». Таким образом можно наглядно представить фильтр любой глубины вложенности логических операций в виде иерархической организационной структуры.

Рыбин П.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ КОМПЛЕКСОМ ПРИГОТОВЛЕНИЯ МНОГОКОМПОНЕНТНЫХ СМЕСЕЙ

В настоящее время на российских предприятиях применяется оборудование и системы управления в основном импортного производства таких производителей как Siemens, Liebherr, ELBA, Simem, ORU, Steel Kamet, Wiggert, Compactors, Tecwill, Stetter, и другие.

В связи с введением санкций и существенным удорожанием импортного оборудования, возникает задача импортозамещения систем управления на основе безопасного программного обеспечения собственной разработки, гарантирующего отсутствие недекларированных программных возможностей, создания более дешевых и ремонтопригодных устройств.

Целью разработки является повышение уровня конкурентоспособности и качества управления предприятиями на основе внедрения программного модуля для автоматизации процесса управления технологическим комплексом приготовления многокомпонентных смесей.

Разрабатываемый программный модуль автоматизации процесса управления технологическим комплексом приготовления многокомпонентных смесей предназначен для обеспечения эффективного функционирования предприятия в соответствии с требованиями ГОСТ 24.103-84.

Модуль имеет интерфейс, который обладает возможностью многофункциональной работы с графическими образами, а также тактильной работы.

В докладе предложен новый подход к оперативному совершенствованию этого интерфейса при помощи специального конструктора, а также новый алгоритм разработки программного модуля, позволяющего существенно сэкономить время на совершение операций по приготовлению смесей в связи с новым графическим интерфейсом.

В отличии от зарубежных аналогов, разработанный модуль имеет возможность непосредственного подключения к ПК по стандартному интерфейсу.

Предусматриваются следующие технические мероприятия по защите информации в разрабатываемом программном модуле:

– осуществляется идентификация и проверка подлинности субъектов доступа при входе в операционную систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

– проводится идентификация и аутентификация субъектов доступа при входе в средство защиты от программно-математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю длиной не менее шести буквенно-цифровых символов, предусмотрены механизмы блокирования доступа к средствам защиты от ПМВ при выполнении трех неудачных попыток ввода пароля;

– осуществляется регистрация входа субъекта доступа в систему, регистрация загрузки и инициализации операционной системы и ее программного останова;

– проводится периодическое тестирование функций системы при изменении программной среды и персонала с помощью тест-программ, имитирующих попытки НСД.

Савельев И.Л., Шерстюк Ю.М.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»

УСТОЙЧИВОСТЬ И БЕЗОПАСНОСТЬ ТЕХНОЛОГИЧЕСКОГО МОНИТОРИНГА СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ

Процесс управления средствами телекоммуникации в сетях спецпотребителей существует в условиях деструктивных внешних и внутренних воздействий. Помимо применения сертифицированных средств СВТ, соответствующих уровню безопасности создаваемой автоматизированной системы управления, подсистема технологического мониторинга должна применять различные принципы построения и функционирования, позволяющие обеспечивать требуемый уровень безопасности и устойчивости процесса управления (мониторинга).

Устойчивость мониторинга обеспечивается следующими методами:

– - разделение средств мониторинга (ТКО) на несколько независимых доменов. Граница деления — узел связи/ подразделение УС. В рамках каждого домена создается (используется) единая система разграничения доступа, идентификации, аутентификации и авторизации субъектов мониторинга. Выход из строя одного домена (УС) не приводит вы ходу из строя всей системы управления;

– все домены образуют единую иерархию управления, УС подразделяются на старшие и младшие, с четко регламентированной системой взаимодействия — старший УС имеет возможность контролировать и управлять средствами подчиненного УС в рамках выделенных ему полномочий. Это позволяет обеспечить процесс управления ТКО подчиненного УС со стороны старшего УС в случае отсутствия на младшем УС персонала надлежащей квалификации.

– настройки смежных УС иерархии планируются с единого центра, размещенного на старшем узле. С этого же центра должна обеспечиваться возможность контроля соответствия настроек подчиненных УС плану;

– в рамках одного УС применяются отказоустойчивые технологии, позволяющие обеспечить непрерывное функционирование технических средств при сбоях и отказах. Отказоустройчивость достигается за счет применения систем бесперебойного питания, резервирования аппаратных средств (УВМ) и применения кластерных технологий при построении программных средств мониторинга.

Обеспечение безопасности целесообразно рассмотреть на двух уровнях: в рамках одного УС и при взаимодействии двух УС между собой.

При управлении в пределах ЛВС УС требуется обеспечить:

– создание контролируемой зоны, доступ из-вне к которой закрывается межсетевыми экранами, т.к. внутри контролируемой зоны трафик межмашинного обмена может передаваться в открытом виде;

– для увеличения безопасности обмена трафиком мониторинга следует применять ТКО, чьи агенты управления поддерживают обмен по протоколу SSL. Это могут быть протоколы HTTPS, SNMP v.3;

– использование механизмов разграничения доступа должно базироваться на единой, в рамках УС, системе идентификации, аутентификации и авторизации. Применяемые программные средства мониторинга должны поддерживать механизмы интеграции с существующей на УС системы разграничения доступа.

При взаимодействии двух УС между собой требуется обеспечить возможность, чтобы трафик, покидающий контролируемую зону должен быть «закрыт» с использованием криптографических программных или программно-аппаратных средств. Это может быть защищенное соединение (протокол SSL) или линейные шифраторы, установленные на границе контролируемой зоны.

Кроме контроля неизменности настроек самой системы управления из единого центра также следует контролировать процесс изменения настроек самого ТКО. Для этого требуется:

– создавать эталонный «слепок» параметров мониторируемого ТКО с возможностью периодического сравнения конфигурации ТКО с ранее сделанным эталоном. В случае расхождения значений параметров система управления должна сигнализировать о несанкционированном изменении и позволять автоматически или автоматизированно восстановить конфигурацию ТКО с использованием эталона;

– формирование единого журнала безопасности, в который необходимо собирать сведения о действиях по изменению настроек системы управления, настроек мониторируемых ТКО, действия операторов системы управления. Данный журнал должен быть доступен только администратору безопасности, чья роль должна обязательного присутствовать с системе управления.

Реализация указанных методов позволит создать систему мониторинга и управления средствами телекоммуникаций, пригодных для эксплуатации на УС спецпотребителей и соответствующих уровню безопасности, применяемых на УС спецпотребителей.

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

ПОВЫШЕНИЕ СТРУКТУРНОЙ СКРЫТНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С ХАОТИЧЕСКИМИ СИГНАЛАМИ

Известно, что в современных системах передачи информации (СПИ) в качестве сигнала переносчика в основном используется гармоническое колебание. Защита информации в таких системах осуществляется на верхних уровнях эталонной модели взаимодействия открытых систем. Использование хаотических сигналов в перспективных СПИ позволит обеспечить их структурную скрытность на физическом уровне.

При этом СПИ, построенные на основе использования хаотических сигналов бывают как с пассивной паузой, так и с активной. При этом сложность технической реализации и устойчивость их работы значительно разница. Наиболее устойчивую работу СПИ с хаотическими сигналами, имеют системы с пассивной паузой, однако при этом они обладают низкой структурной скрытность.

Поэтому целью доклада является, раскрыть СПИ с хаотическими сигналами обладающую повешенной структурной скрытностью, при простой технической её реализации.

В описываемой СПИ с хаотическими сигналами используется записанная в накопитель копия хаотической структуры сигнала с требуемыми характеристиками, используется как на передающей, так и на приемной стороне. При этом СПИ с хаотическими сигналами состоит из: источника информации, модулятора – передатчика, накопителя хаотических сигналов, канала связи, полосового фильтра, усилителя, умножителей, инвертора, интеграторов, вычитающего устройства, решающего устройства, получателя информации.

Процесс передачи информации осуществляется следующим образом. После вхождения приемной и передающей части системы в синхронизм, она осуществляет передачу информации с использованием хаотического сигнала, который воспроизводятся с накопителя копии хаотического сигнала. После поступления от источника информациисигнал, модулируется хаотическим сигналом по закону информационного сигнала и передаётся в канал связи.

Детектирование информационного сигнала на приёмной стороне осуществляется путём его параллельного умножения на копию хаотического сигнала и последующего интегрирования. Причём, на второй умножитель хаотический сигнал поступает через инвертор. Затем происходит их вычитание в вычитающем устройстве, после чего он поступает в решающее устройство, где происходит сравнение принятых уровней с пороговым значением напряжения. С выхода решающего устройства информация поступает к получателю информации.

Если злоумышленник, с целью выделения информации, попробует воспользоваться энергетическим приёмником то поступившая на его вход непрерывная хаотическая последовательность, будет проинтегрирована по мощности, и в пределах длительности интервалов

отсчёта, будет выделена энергия принятого хаотического сигнала, но последующий её статистический анализ не позволит выделить структуру информационного сигнала.

Подводя итог можно сказать, что при использовании предложенной СПИ с хаотическими сигналами структурная скрытность будет повешена пропорционально «сложности» используемой структуры сигнала.

Синещук М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ МЧС РОССИИ

Распределенные вычислительные сети (РВС) - один из самых чувствительных элементов информационных систем (ИС), с точки зрения надежной и безопасной работы. Предоставляемые ими услуги практически полностью создаются на основе ИТ-решений.

Так как на сегодняшний день РВС имеют высокую оснащенность средствами обеспечения информационной безопасности (ИБ), на первый план выходят решения, позволяющие оптимизировать и автоматизировать процессы ИБ, повысить управляемость, обеспечить прозрачность, легитимность и катастрофоустойчивость РВС.

Наличие большого числа разнообразных ИС, используемых в МЧС России, приводят к тому, что традиционные способы управления правами доступа к ИТ-решениям в РВС становятся неэффективными с точки зрения безопасности и затрат ресурсов. Сегодня важно уметь контролировать и оперативно управлять всеми процессами ИБ, поддерживать требуемый уровень ИБ в режиме реального времени, что предусматривает проведение оценки рисков ИБ.

Стандарты в области управления ИБ (ISO IEC 17799; ISO IEC 27001; BS 7799-3; NIST 800-30), выделяют общую для всех модель оценки рисков ИБ, где риск можно рассматривать как функционал угрозы: Risk=f(U). Для РВС необходимо применять более детальный анализ рисков ИБ, который осуществляется с помощью построения модели ИС, с рассмотрением средств защиты ресурсов, взаимосвязи ресурсов между собой, влияния прав доступа групп пользователей, организационных мер.

В ходе анализа должны быть получены следующие данные:

- инвентаризация ресурсов;
- значения риска для каждого ценного ресурса организации;
- значения риска для ресурсов после задания контрмер (остаточный риск);
- эффективность контрмер;

рекомендации экспертов по устранению уязвимостей системы ИБ.

Результаты оценки рисков нарушения ИБ должны документально фиксироваться.

В настоящее время для анализа рисков ИБ применяют системы, которые позволяют оценить существующие в системе риски и выбрать оптимальный по своей эффективности вариант защиты. Чаще всего данный расчёт проводят на основе соотношения существующих в системе рисков к затратам на ИБ. Данную задачу решают программные комплексы, разработанные для анализа и контроля информационных рисков - это британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch), российский ГРИФ (компания Digital Security) и АванГард (Институт системного анализа РАН).

Все методики, применяемые в данных программных продуктах, условно можно разделить на следующие три вида:

– методики, использующие оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). К таким методикам, в частности, относится FRAP;

– количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;

– методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

Построение моделей рисков позволяет оценить опасность каждой из угроз и определить приоритетность мер по защите автоматизированных ИС и развитию подсистем ИБ. Наиболее важные из указанных угроз будут образовывать модель значимых угроз ИС. Таким образом, решаются задачи первого этапа контроля и планирования развития защиты автоматизированных ИС.

Следующим этапом является определение возможностей по защите и планирование конкретных мероприятий. По каждой из выявленных угроз может быть определен целый перечень требований, которые необходимо выполнить для того, чтобы добиться ее устранения, и перечень мероприятий, с помощью которых можно добиться выполнения этих требований.

В то же время, некоторые мероприятия могут обеспечивать защиту более чем от одной угрозы. Поэтому необходимо провести анализ по критерию "эффективность-стоимость" всех возможных комплексов мероприятий и, при необходимости, решить задачу выбора наиболее эффективного комплекса.

В сфере ИБ РВС оценка рисков играет первостепенную роль. Из-за неадекватной оценки рисков, связанных с осуществлением угроз ИБ в современном высокотехнологичном обществе, дискредитируются мероприятия, обеспечивающие ИБ, а государство, ведомства и отдельные потребители услуг несут весьма ощутимый ущерб.

Синещук Ю.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

КИБЕРБЕЗОПАСНОСТЬ И ПРОБЛЕМЫ ОПЕРАТИВНОЙ АДАПТАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ МВД РОССИИ.

За последние годы в мире и в нашем государстве многое изменилось в плане совершенствования методов, способов борьбы с организованной преступностью и террором. Сегодня эта деятельность неразрывно связана с процессами глобальной информатизации всех сторон и аспектов жизнедеятельности МВД. Это выражается, с одной стороны, – в стремительном росте объема производимых и потребляемых информационных ресурсов, а с другой, – в широком использовании современных информационных технологий в оперативно-служебной деятельности органов внутренних дел, обеспечивающх повышение эффективности управления путем автоматизации таких процессов как:

– сбор, обработка и хранение информации о возможностях и реальном состоянии сил и средств органов внутренних дел МВД России, поступающей из различных источников;

– моделирование контртеррористических/специальных операций;

– проведение различных расчетов;

– выдача руководителям органов (командирам подразделений) и органам управлений (штабам) справочной информации, необходимой для своевременной подготовки научно обоснованных решений;

– планирование действий в соответствии с принятым решением;

– корректировка планов применения сил;

– своевременное доведение (отмена) приказов (команд, сигналов), и распоряжений и контроль их исполнения и др.

Вместе с тем научно-технический прогресс, создание и глобальное распространение электронных технологий, особенно сети Интернет, стало основной причиной появления и распространения киберугроз. Сегодня техническими возможностями компьютеров, их программным обеспечением, сетью Интернет, сотовой связью стремятся воспользоваться криминальные элементы, количество которых с каждым днем возрастает. По мнению специалистов, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете.

Именно поэтому в деятельности МВД значительное внимание уделяется проблеме борьбы с киберпреступностью, действиям в условиях информационного противоборства. Кибербезопасность сегодня рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества.

В настоящее время данные обстоятельства предопределяют доминирование информационной составляющей в структуре профессиональной деятельности специалиста МВД России. Владение современными информационными технологиями становится главным критерием и залогом эффективной профессиональной деятельности сотрудников ОВД на любом посту и в любой должности. В конечном итоге это влечет за собой качественное изменение как самого характера профессиональной деятельности специалиста органов внутренних дел Российской Федерации, так и требований к уровню его профессиональной подготовки.

Направления, содержание и объемы подготовки специалистов по вопросам применения информационных систем и технологий, обеспечения информационной безопасности на государственном (ведомственном) уровне определяются:

– степенью уязвимости государства в информационном пространстве (киберпространстве);

– степенью понимания угроз информационной безопасности, с соответствующей адекватной реакцией органов государственного (ведомственного) управления;

– определенными задачами кадрового обеспечения существующих и перспективных структур, отвечающих за информационную безопасность личности, общества и государства.

При этом возникает острая необходимость оперативной адаптации образовательной деятельности высших учебных заведений МВД, к общенациональным интересам в сфере образования, основанным на общих тенденциях мирового развития, обуславливающих переход к информационному обществу.

Исходя из этого, в настоящее время основной акцент в системе профессиональной подготовки специалистов МВД России должен делаться на формирование профессионально подготовленных защитников правопорядка, способных эффективно действовать в динамично меняющейся информационной среде, применяя новейшие разработки в области науки и техники, позволяющие эффективно противодействовать как традиционной, так и высокотехнологичной преступности.

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

МЕТОДОЛОГИЯ ОТКРЫТОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ СЕТИ ТРЕХ КОРРЕСПОНДЕНТОВ

Исследованы модели и методы процесса формирования общего ключа трех корреспондентов связи по открытым каналам связи в условиях прямой передачи последовательностей символов. Произведена постановка задачи формирования ключа трех корреспондентов связи по открытым каналам связи. Предложена модель канальной связности (МКС) в рамках которой приведено математическое описание источника выполнено разделение на каналы корреспондентов и канал перехвата (КП) нарушителя *E*.

Для передачи информации предлагается использовать разработанные модели случайного кодера, а на приемной стороне - детерминированного декодера. В этом случае выход КП для нарушителя представляется случайным выбором сообщения источника (определяется случайным выбором кодового слова из кодового подмножества) и равномерным законом распределения вероятностей принятой последовательности символов на входе КП при условии выбора сообщения источником. В общем виде для достаточно большой длины выбранного кодового слова представлена последовательность действий, выполняемых корреспондентами для формирования ключа (К).

В основе предлагаемого метода оценки формирования ключа трех корреспондентов связи по открытым каналам связи предложены основные локальные показатели качества ключа, определяющие его безопасность, своевременность и достоверность. Качественно показатели качества сводятся к надежной передаче большого количества бит «хорошего» К при малой утечке информации к нарушителю. Введена «информационная» скорость формирования К трех корреспондентов, представляющая собой удельное количество информации ключа приходящееся на один канальный символ. Сформулированы и обоснованы локальные требования к К. Введены понятие ключевой пропускной способности трех корреспондентов и терминология процесса формирования ключа.

Совокупность, включающая разработанную модель канальной связности, выполнение во времени шагов по формированию К представляется как процесс формирования К трех корреспондентов связи. Основным параметром выбрана ключевая пропускная способность, которая определяет асимптотическую эффективность по оперативности формирования К трех корреспондентов по открытым дискретным каналам связи при заданных соотношениях вероятностей ошибок в каналах связи корреспондентов и канале перехвата.

Задача исследования определяется поиском ключевой пропускной способности для максимально возможной скорости подбираемого кода. Сформулирована и доказана теорема о ключевой пропускной способности. Найдены граничные значения и выполнена оценка ключевой пропускной способности процесса формирования ключа трех корреспондентов связи при прямой передаче для общего двоичного алфавита. Полученные результаты оценки позволили выявить закономерность, определяющую возможность успехаформирования К отвечающего требованиям, если оценка суммы числовых значений вероятностей ошибок в составляющих каналах корреспондентов будет меньше оценки вероятности ошибки в КП.

Особенностью исследований формирования К в условиях прямой и обратной передач последовательностей символов явилось преобразование исходной модели связности, к «виртуальной», которое не ухудшает качества «виртуального» информационного обмена между корреспондентами и ухудшает качество «виртуального» КП нарушителя.

Исследования асимптотической эффективности определили условия преимущественного использования вышеописанных моделей открытого ключевого согласования.

Полученные результаты проведенных исследований в полном объеме характеризуют процесс открытого ключевого согласования сети минимального числа корреспондентов. Они не противоречат и взаимосвязаны с известными ранее результатами исследований, полученными другими авторами и могут быть использованы для синтеза системы открытого формирования ключа сети связи, включающей большое количество корреспондентов.

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

МОДЕЛЬ БЕЗОПАСНОГО ФОРМИРОВАНИЯ СЕТЕВОГО КЛЮЧА

Предлагается теоретическая модель установления криптосвязности сетевых корреспондентов по открытым каналам связи, которая определяет концептуальные основы открытого сетевого ключевого согласования.

Актуальность построения подобной модели определяется наличием противоречия между высокой потребностью закрытого обмена информацией большого числа сетевых корреспондентов и низкой устойчивостью сетевого ключа к различным атакам нарушителя.

Теоретическая модель включает объект и предмет исследования, систему понятий и категорий, исходный теоретико-информационный базис и концептуальную модель. Последняя в свою очередь включает модель открытой передачи информации в сети связи, модель перехвата информации нарушителем, модель открытого сетевого ключевого согласования, модель оценки эффективности, модели, методы и методики открытого ключевого согласования сети минимального числа корреспондентов. Определены место предлагаемой модели среди других теорий, а также принцип формирования системы понятий.Теоретическую модель можно рассматривать как дальнейшее развитие концепции «подслушивающего канала» А. Вайнера и существенно расширяет последнюю.

Предложенная модель передачи информации в сети связи из N корреспондентов представляется моделью процесса передачи информации в сети связи посредством N широковещательных каналов связи. Приведено математическое описание процесса передачи информации по широковещательным каналам связи от различных источников сообщений. Обоснован выбор единой модели алгоритма линейного шифрования.

Разработанная модель перехвата информации нарушителем в сети связи представляется совокупностью каналов перехвата нарушителя. Нарушитель способен перехватить всю информацию, передаваемую в сети связи. Его целью является определение (получение, вычисление, перехват и т.д.) формируемого корреспондентами сети связи сетевого ключа. Ограничениями корректно выбраны предположения о пассивности нарушителя и ограниченности его ресурса. В качестве допущений сделано предположение о том, что нарушителю достоверно известны полное описание процессов генерации, передачи, хранения и обработки информации, порядка, содержания и параметров реализации процедур, выполняемых корреспондентами для формирования сетевого ключа. Кроме этого предполагается, что нарушителю полностью известны статистические характеристики множеств генерируемых сообщений, формируемых ключей, широковещательных каналов связи.

В предлагаемой модели открытого сетевого ключевого согласования разработаны и всесторонне исследованы методыоткрытого сетевого ключевого согласования: метод «широковещательного» формирования сетевого ключа и метод «пересекающихся групповых ключей». Проведенный анализ представленных методов формирования сетевого ключа показал, что наиболее отвечает требованиям открытого формирования сетевого ключа второй метод, который выбран в качестве базового. Исследованы условия реализации выбранного метода.

Отсутствие известных результатов научных исследований в области теории и практики открытого ключевого согласования сети минимального числа корреспондентов актуализировало проведение исследований процесса открытого ключевого согласования в группах из трех корреспондентов, связанных между собой открытыми каналами связи с ошибками.

Разработана модель оценки эффективности, включающая систему показателей качества, систему требований, показатели эффективности формирования сетевого ключа. Описан порядок оценки эффективности.

Сделано предположение о том, что использование предлагаемой модели создаст условия для адекватного описания и проведения исследований процессов как установления новой, так и восстановления потерянной криптосвязности сетевых корреспондентов по имеющимся открытым каналам связи.

Сныткин И.И., Кулюпин Е.Н.,
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

РЕАЛИЗАЦИЯ МЕХАНИЗМА И УСЛУГ ЗАЩИТЫ ИНФОРМАЦИИ (ШИФРОВАНИЕ ПОТОКА ТРАФИКА СОГЛАСНО ГОСТ РИСО 7498) НА 1-М УРОВНЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ ISO НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМНЫХ СВОЙСТВ И ХАРАКТЕРИСТИК ПРОИЗВОДНЫХ УПРАВЛЯЮЩИХ ЧИСЛОВЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Основой методов и средств защиты информации, в частности, циркулирующей по открытым системам, являются требования ГОСТ Р ИСО/МЭК 7498. Данный стандарт, ориентируясь на 7-ми уровневую базовую модель логической структуры информационных систем, установленных протоколом X.25 ISO,определяет услуги и механизмы их защиты,а также устанавливает основы для обеспечения скоординированных разработок действующих и будущих стандартов по взаимосвязи открытых систем (ВОС), т.е. он в целом охватывает общие вопросы защиты процесса защиты обмена данными на логических уровнях базовой эталонной модели ВОС.

Особо отмечается гибкость стандарта, определяющего, в том числе, и направления развития технических средств приема/передачи данных. Однако при всем при этом в настоящее время отсутствует какая-либо регламентирующая (нормативно-правовая) база документов, которая раскрывала бы способы реализации предписанных механизмов защиты. В частности, на 1-м (физическом) уровне базовой эталонной модели ВОС услуга защиты установлена в виде полного шифрования потока данных за счет расширения частотного спектра,т.е. предполагается процедуру

«шифрования» трафика базировать на применении широкополосных шумоподобных сигналов (ШШС). Однако таким образом такое «шифрование» к шифрованию как таковому не имеет отношения, а предполагает, что расширение спектра обеспечивает борьбу с сосредоточенными по спектру узкополосными помехами и т.п., хотя реальное шифрование некриптографическим путем можно и реализовать, используя ШШС. Так в докладе предлагается это делать на основе использования сигналов ППРЧ в виде кодовых дискретно-частотных сигналов (КДЧС).

Применение метода ППРЧ любой реализации делает используемые сигналы широкополосным шумоподобными. Этот метод наиболее эффективен и устойчив в тех телекоммуникационных сетях, где используются высокочастотные участки КВ, УКВ и СВЧ-диапазоны электромагнитных волн вследствие отсутствия замираний и многолучевости в данных диапазонах. Таким образом, кроме расширения спектра частот, будет обеспечиваться повышение помехозащищенности, криптоустойчивости и имитостойкости процесса передачи данных.

В ряде работ предложены правила построения КДЧС на основе УЧКП как мультипликативных группах в простых полях Галуа GF(p). Однако такие УЧКП имеют существенные недостатки: не высокие ансамблевых характеристик УЧКП при фиксированном модуле p; сравнительно не большое число различимых значений корреляционных функций УЧКП по заданному модулю p; сложное техническое формирование УЧКП больших длительностей; попытки увеличения объема ансамбля УЧКП по заданному модулю p за счет циклических перестановок (сдвижек) в их тонкой внутренней структуре, с практической точки зрения, следует рассматривать как элементарную «задержку»; теоретические не исследованы и практически не применяются свойства детерминированности УЧКП.

В связи с этим, предлагается использовать другой подход в реализации УЧКП - в построении больших квазиоптимальных композиционных систем, объединяющих в себе по заданному алгоритму два или более ансамбля УЧКП, т.е. так называемых производных управляющих числовых кодовых последовательностей (ПУЧКП). Применение ПУЧКП, в первую очередь, обуславливается возможностью построения максимальных объемов кодовых форм при фиксированных необходимых длительностях компонент, что необходимо для «закрытия» каждого бита передаваемой информации неповторимой на сеансе связи ПУЧКП. А проведённые машинные эксперименты исследования корреляционных свойств и характеристик ПУЧКП показывают, что изложенные разработанные положения по ПУЧКП потенциально позволяют выйти за рамки ГОСТа Р ИСО/МЭК 7498, но только для улучшения помехозащищенности, криптоустойчивости и имитостойкости процесса передачи данных 1-м (физическом) архитектуры информационных систем.

Сныткин И.И., Кулюпин Е.Н., Сныткин Т.И.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
Москва, 27 Центральный научно-исследовательский институт Министерства обороны Российской Федерации

НЕКРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СПОСОБЫ РЕАЛИЗАЦИИ МЕХАНИЗМОВ И УСЛУГ ЗАЩИТЫ ИНФОРМАЦИИ В ТРАНСПОРТНОЙ ПОДСИСТЕМЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В специальныхтелекоммуникационныхсистемах (системах связи,системах передачи данных, др.) основной путь защиты информации (ЗИ) реализуется за счет специального уровня защиты информации, который использует методы криптографии и засекречивания различных видов информации. Организационно-техническое обеспечение функционирования данного специального уровня осуществляется государственными органами и службами, которые призваны прежде всего обеспечить недопущение несанкционированного доступа (НСД) к конфиденциальной информациии ее использования. Учитывая возможность современного агентурного воздействия на организационно-техническое обеспечение системы НСД со стороны противника, а также возможности этих воздействий на сам процесс обмена конфиденциальностей информацией после «снятия» криптографической защиты на пользовательских уровнях логической структуры архитектуры открытых систем (5-,6-,7-й уровни), в настоящее время можно говорить о том, что эффективность и надежность, с точки зрения обеспечения указанной конфиденциальности, заметно снизилась. В этой связи, а также с учетом современных требований по выполнению ГОСТ Р ИСО/МЭК 7498 становится весьма актуальным необходимость разработки необходимых эффективных процедур ЗИ на каждом логическом уровне архитектуры информационных систем (и открытых и закрытых). Указанным ГОСТом в принципе определены системные механизмы и услуги ЗИ на каждом логическом уровне, однако даже предполагать, что такие услуги и механизмы должны строиться на основе использования известных криптографических методов и средств является несостоятельным, так как это само по себе будет предполагать расширение соответствующих организационно-технических структур известных органов и соответствующее удорожание процесса ЗИ. Поэтому естественно, что на повестку дня выносится проблема организации и создания услуг и механизмов ЗИ на всех уровнях логической структуры согласно ГОСТа некриптографическими методами. В докладе рассматриваются

возможные реализуемые методы по отношению к логическим уровням транспортной системы (ТС) (1-, 2-, 3, 4-му уровням логической структуры). Основой данных методов является широкое применение свойств скрытности, имитостойкости, криптоустойчивости, которыми обладают сложные сигнально-кодовые конструкции (ССКК) нелинейной структуры (НС). Основной путь для решения данных задач является реализация функций и задач всех уровней на основе применения ССКК НС. Так, например, в докладе рассматривается построение таких методов: на 1 уровне - за счет применения ССКК НС в виде кодовых дискретно-частотных сигналов (КДЧС), строящихся на основе управляющих числовых кодовых последовательностей (УЧКП), производных управляющих числовых кодовых последовательностей (ПУЧКП) в конечных полях Галуа GF(p) и применения принципа передачи открытых ключей Диффи–Хелмана в процессе информационного обмена, и ССКК НС в виде ФМ-ПСП, в качестве которых выступают нелинейные и производные нелинейные рекуррентные последовательности (НЛРП и ПНЛРП); на 2-м уровне – за счет применения ССКК НС в виде систем НЛРП и ПНЛРП для решения задач устойчивых и ускоренных поиска, обнаружения, приема, тактовой и цикловой синхронизации, обработки информации; на 3-,4-м уровнях логической структуры в интересах адресации и маршрутизации и устойчивого обмена информации - за счет использования систем ССКК в виде НЛРП и ПНЛРП. В основе этих методов не лежат в прямой форме организационно-технические мероприятия, характерные для классических криптографических методов, однако некоторые сущностные элементы этих методов, такие как: смена ключевых данных, поточное гаммирование и др., - реализуются в некриптографических методах косвенно или опосредованно. В докладе рассматриваются возможно достигаемые системные параметры и характеристики ЗИ (в виде математических соотношений, графиков и таблиц) за счет применения некриптографических методов на каждом уровне логической структуры ТС. Делаются выводы об эффективности таких методов и намечаются пути их реализации.

Сныткин И.И., Кулюпин Е.Н., Сныткин Т.И.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
Москва, 27 Центральный научно-исследовательский институт Министерства обороны Российской Федерации

МЕТОД УСКОРЕННОГО ПРИЕМА И СИНХРОНИЗАЦИИ ПРОИЗВОДНЫХ НЕЛИНЕЙНЫХ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ КАК «ТРЕТЬЯ РЕШАЮЩАЯ СХЕМА» ЭФФЕКТИВНОГО РАДИОПРИЕМА

В докладе рассматриваются результаты исследований по разработке теории «третьей решающей схемы» (ТРС) радиоприема по обеспечению ускоренного приема (поиска, обнаружения, синхронизации, обработки) шумоподобных широкополосных сигналов (ШШС) на основе фазоманипулированных псевдослучайных последовательностей (ШШС, ФМ-ПСП) в виде производных нелинейных рекуррентных последовательностей (ПНЛРП).

Разработанные элементы теории «третьей решающей схемы» (ТРС) показывают: а) ТРС есть процедура приема в режимах поиска, обнаружения, синхронизации и обработки производных нелинейных рекуррентных последовательностей (ПНЛРП) по принятию решения о структуре ПНЛРП и, следовательно, о сообщении (элементарном), на основе анализа и идентификации структуры детерминированной корреляционной функции (КФ) двукратной ПНЛРП (ДК ПНЛРП); б)ТРС реализует свои функции как схема разнесенного приема по форме и структуре КФ ПНЛРП и может реализовываться как «фактор-шлюз» между 1-м и 2-м, 2-м и 3-м уровнях базовой модели логической структуры информационных систем, и возможно, другими уровнями при использовании ПНЛРП или других псевдослучайных последовательностей (ПСП), имеющих детерминированную структуру КФ; в) ТРС может являться как единственным и самостоятельным вариантом процедуры приема широкополосного шумоподобного сигнала (ШШС), так и параллельным (или дополнительным) «каналом-процедурой» приема; г) разработанные математические аппараты построения, реализации и оценки качества в виде четырех аналоговых режимов принятия решений ТРС и пяти дискретных методов принятия решений ТРС позволяют сформулировать, математически описать и оценить качества выше указанных режимов и методов принятия решений ТРС, показывающие высокий уровень эффективности ТРС, а именно: только для значений длительностей порождающих компонент ПНЛРП l_1 и l_2, равных 7 и 11(например, для пяти дискретных методов принятия решений ТРС), обеспечивается выигрыш в помехоустойчивости, ускорения поиска и синхронизации от 3-х до 8-ми порядков).

Разработанные аналоговые режимы и дискретные методы принятия решений ТРС помимо всего прочего увеличивают и пропускную способность информационного канала, за счет вышеуказанного выигрыша в помехоустойчивости приема, ускорения поиска и синхронизации.

Полученные результаты исследований являются непосредственно теоретической, научно-методической, технической и практической основой, совокупностью рекомендаций, технических решений, позволяющих проводить научно-техническое обоснование путей и методов построения и реализации, непосредственно проектировать и разрабатывать перспективную ТРС и ее

динамические адаптивные протоколы передачи. Внедрение данных научных и практических результатов в интересах построения и реализации пакетных радиосетей сбора и обработки информации автоматизированных систем обеспечит высокую степень оперативности, устойчивости, скрытности, имитостойкости в условиях активных радиоэлектронной борьбы и информационного противоборства.

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

СИТУАЦИОННОЕ ИНТЕЛЛЕКТУАЛЬНО-АГЕНТНОЕ МОДЕЛИРОВАНИЕСИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ

Во вводной части доклада рассматриваются вопросы построения ситуационных интеллектуально-агентных систем моделирования систем защиты (СЗ) на примере корпоративных информационных сетей (КИС) с поддержкой качества обслуживания. Рассматриваются мультиагентная интеллектуальная СЗ (МИСЗ), приводится теоретико-множественное описание агентов и их взаимодействий.

Главным отличием современных интеллектуальных СЗ является их распределенность, обеспечение качества обработки и применение распределенных знаний. Главный смысл происходящих в настоящее время смен концепций (парадигмы) создания и использования средств искусственного интеллекта – переход от предположений, справедливых только для изолированных систем искусственного интеллекта, от индивидуальных систем к распределенной обработке информации и разработке МИСЗ.

При практической реализации распределенных МИСЗ возникли серьезные трудности с проектированием и описанием объединенных в единую сеть разнородных локальных компьютерных узлов. Только при применении теории интеллектуально-агентных систем возможно преодолеть трудности с моделированием разнородных КИС с разнообразным оборудованием.

Исходя из многоуровневой структуры ситуационного моделирования, авторы считают, что необходима МИСЗ, которая формирует взаимодействие интеллектуальных агентов (ИА) на всех стратах моделирования. Для структуры ситуационного моделирования налицо все признаки многоагентных систем: распределенность, независимая параллельная работа экспертов, масштабируемость, т.е.при добавлении нового объекта или подсети система не перепрограммируется, а только добавляются новые агенты и включается в общее взаимодействие.

На основании изложенных выше соображений о характеристиках известных моделей ИА и изложенной формальной теории ситуационного моделирования, авторы предлагают определить ИА как гибридную архитектуру. Интеллектуальный агент в системе будет представляться в виде МИСЗ, что позволит разрабатывать иерархию функций, процессов, моделей и взаимосвязей в виде отдельных взаимосвязанных агентов]. Такой подход позволяет разрабатывать независимо модель каждого агента, определять его роль в МИСЗ и его взаимосвязи с другими агентами. Такой принцип хорошо встраивается в концепцию построения системы ситуационного интеллектуального-агентного моделирования.

В итоге можно констатировать, что доклад посвящен реализации обобщенной модели построения систем ситуационного интеллектально-агентного моделирования КИС с поддержкой качества обслуживания. На основе предложенной интеллектуальной концепции ситуационного моделирования появляются новые возможности при моделировании сетей, анализе их функционирования и уменьшение влияния человеческого фактора при возникновении сложных ситуаций в реальных системах. Результатом функционирования системы ситуационного интеллектуального-агентного моделирования является управляющие действия в зависимости от развития ситуаций. Изложенный подход представляет собой развитие идеологии ситуационного управления для реализации распределенных систем защиты информации.

Таран В.В., Шерстюк К.Ю., Шерстюк Ю.М.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

ФУНКЦИОНАЛЬНЫЕ ПОДСИСТЕМЫ И ПРОФИЛИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В АСУС

По своей сути система управления защитой информации (СУЗИ) в автоматизированной системе управления связью (АСУС) представляет собой функциональную интеграцию двух систем:

– системы планирования (включая документальное оформление его результатов);

– контрольно-сигнальной системы событийного и параметрического оперативного контроля и ретроспективного анализа интегрируемых разнородных данных мониторинга, предоставляемых средствами защиты информации, а также функциональными службами АСУС (включая их механизмы контроля и регистрации доступа).

Объективно СУЗИ АСУС являясь территориально и организационно распределенной, должна формировать единый автоматизированный контур планирования защиты информации, контроля информационной безопасности, интегрирующий и дополняющий существующие средства защиты в составе АСУС.

Основными целями создания и внедрения СУЗИ являются:

– обеспечение объективной оценки степени информационной безопасности управляемого телекоммуникационного оборудования и АСУС в целом;

– оптимальное (рациональное) распределение средств защиты для обеспечения устойчивости сети связи, управляемой АСУС, в условиях действия деструктивных и дестабилизирующих факторов (компьютерных атак);

– повышение оперативности и обоснованности управляющих воздействий на систему и отдельные средства защиты информации, упрощение действий по их конфигурированию, контролю функционирования и аудиту мониторируемых ими событий.

Распределенность СУЗИ в иерархической системе пунктов управления АСУС обеспечивается автоматическими и автоматизированными (по явному запросу пользователя) информационными взаимодействиями посредством механизмов проксирования и сбора данных.

Под проксированием понимается возможность доступа клиентского приложения к удаленному серверу службы – через механизм проксирования, предоставляемый сервером службы, локальным по отношению к пользователю.

Под сбором данных понимается периодическая автоматическая передача предусмотренных данных от одного программного сервера к другому. Автоматический сбор данных может иметь как локальный, так и сетевой характер.

Распределенная СУЗИ имеет иерархическую структуру, повторяющую структуру иерархии пунктов управления АСУС. Ее архитектуру определяют:

– функциональные подсистемы – информационная, технологическая и аналитическая;
– обеспечивающие профили и подсистемы СУЗИ:
– профиль информационной безопасности (защиты информации);
– подсистема администрирования, оперативного контроля и управления;
– подсистема информационного обмена;
– обеспечивающие сервисы.

Средства каждого уровня в общем случае обеспечивают как сервисы (услуги) конечного пользователя, так и сервисы для средств своего и более высоких уровней.

Информационная подсистема должна предоставлять сервисы учета средств защиты информации, планирования их применения.

Технологическая подсистема должна предоставлять сервисы оценки обстановки, мониторинга средств защиты информации и управления их функционированием.Аналитическая подсистема должна предоставлять сервисы ретроспективного анализа функционирования СУЗИ, ее средств защиты информации на основе поиска инцидентов в фактографических данных.

Соотнесение распределения задач функциональных подсистем СУЗИ с подразделениями, осуществляющими эксплуатацию сети связи на разных уровнях ее организационно-территориального и функционального деления, определяет содержание процессов функционирования СУЗИ, участие в них должностных лиц органов и пунктов управления АСУС, их полномочия и зоны ответственности, и является основой для формирования детальной функциональной, организационной, информационной и технической архитектуры СУЗИ.

Труфанов С.К.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

ПОИСК ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПО ДАННЫМ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИЙ

В процессе мониторинга сети связи и ее элементов осуществляется сбор сведений о параметрах функционирования, состоянии телекоммуникационного оборудования, а также событий, формируемых оборудованием и средствами автоматизированной системы управления. В целях контроля безопасности системы связи получаемые сведения целесообразно подвергать оперативной обработке, направленной на обнаружение атак или их последствий. Одной из задач такой обработки является поиск инцидентов безопасности —выявление единичных или серийных событий в территориально распределенной системе, указывающих на возможное нарушение информационной безопасности на объектах связи.

Получаемые сведения являются исходными для анализа обстановки и позволяют определить осуществлявшийся к телекоммуникационному оборудованию доступ, изменения параметров и состояний сетевых элементов, происходившие на узлах и коммуникациях сети процессы. В ходе поиска инцидентов можно установить легитимность тех или иных действий с точки зрения политики безопасности, а также их характер. Таким образом, в ходе поиска инцидентов происходит выявление

потенциальной или уже реализованной угрозы. Обнаружение инцидентов позволяет определить уязвимости элементов телекоммуникационной сети, способные привести к ее неработоспособности.

В качестве механизма осуществления поиска инцидентов предлагается использовать механизм назначения сценариев атак — постоянно выполняющихся с заданной периодичностью процедур обработки поступающих данных на основе некоторого типового шаблона. Типовой шаблон является описанием угрозы какого-то одного конкретного типа и с заданными параметрами является основой для функционирования системы обнаружения атак. В качестве параметров при формировании определенного сценария могут выступать частота некоторых событий на заданном временном интервале, возникновение событий определенного класса как на отдельных объектах связи, так и на всей сети, возникновение определенных событийных последовательностей. Для выявления различных угроз следует задавать некоторое динамически пополняемое множество шаблонов, формируемое по результатам анализа функционирования и выявления возможных угроз. Таким образом, первой важной задачей при создании механизма поиска инцидентов ИБ является задача создания набора шаблонов, описывающих максимально обширный спектр потенциальных угроз.

Периодичность выполнения сформированных сценариев определяется критичностью тех или иных элементов системы связи, а также требованиями по эксплуатации.

В ходе выполнения поиска инцидентов информационной безопасности формируется ряд новых событий, информирующих должностных лиц, отвечающих за обеспечение информационной безопасности, о возможных угрозах, что позволяет их своевременно обнаруживать и тем самым повышать эффективность работы средств защиты информации.

Удалов В.С., Гаскаров В.Д.
Россия, Санкт-Петербург, ФБУ «Администрация «Волго-Балт», Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СУДОПРОПУСКА ЗА СЧЕТ ИНТЕРГАЦИИ СИСТЕМ ПОЗИЦИОНИРОВАНИЯ И ВИДЕОНАБЛЮДЕНИЯ

При непрерывном пропуске судов через судоходные шлюзы диспетчеры сталкиваются с проблемой формирования очередности шлюзования судов в направлениях вверх и вниз по течению реки. В связи с этим возникает необходимость информировать судоводителей о приемлемой скорости движения судна по направлению к шлюзу, а также об очерёдности шлюзования и ожидании у причальных стенок, в подходных каналах или на рейде. Для автоматизации процесса судопропуска необходимо иметь точную информацию о позиционировании судна, его скорости, особых условиях шлюзования и т.д., эту информацию можно получать посредством АИС, а так же от служб диспетчерского регулирования движения флота. Эта информация позволяет формировать очередь и осуществлять её обслуживание, до захода судна в камеру шлюза.

Отдельной задачей может являться позиционирование судна непосредственно в шлюзовой камере. Для этого можно использовать системы видеонаблюдения, которые установлены в камере, но используются лишь для визуального контроля процесса шлюзования. Совместив программное обеспечение систем видеонаблюдения с программными средствами позиционирования судов в подходных каналах и в камере шлюза, можно в большей степени автоматизировать и процесс шлюзования, что повысит безопасность судопропуска за счет снижения нагрузки на диспетчера и повышения точности позиционирования

Современные программные средства, интегрированные в процесс управления шлюзованием, помогут существенно облегчить работу оперативного персонала шлюзов за счет снятия с него существенной части задач. Программные продукты, которые могут быть объединены в единый комплекс с целью снижения времени простоя судов в ожидании шлюзования в настоящее время существуют разрозненно и не реализуют заложенный в них потенциал. В это время работают люди, которым свойственна усталость от длительной напряженной работы, время принятия решений и качество этих решений напрямую зависят от их эмоционального состояния. Все это создает условия для возникновения ошибок связанных с «человеческим фактором», что не может позитивно сказываться на безопасности судопропуска.

Программа не устанет от длительной нагрузки, качество и время принятия решений не будет искажено психологическим состоянием оператора, кроме того количество ошибок в расчетах программы значительно ниже, чем у человека. Переложив ответственность за принятие решений о формировании очереди на шлюзование с диспетчера (начальника вахты) шлюза на программные средства вычисления, можно не только повысить безопасность пропуска судов через судоходные шлюзы, но и повысить качество работы человека, который наблюдает за этим процессом и контролирует его. Кроме повышения безопасности есть еще один немаловажный плюс в адаптации режима работы судоходного шлюза к интенсивности судопотока - снижение времени ожидания судов очереди на шлюзование, что повысит пропускную способность отдельного участка русла реки и в перспективе минимизирует очереди на шлюзование, что повысит привлекательность речных грузопассажирских перевозок снизив затраты судовладельцев, связанные с временем простоя флота.

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

АВТОМАТИЗАЦИЯ ВЫБОРА ПОКАЗАТЕЛЕЙ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В быстро меняющемся мире информационных технологий возникает необходимость автоматизации процесса комплексного мониторинга и детального прогноза сетевой обстановки. Задача мониторинга должна решаться на основе применения современных средств ИКТ. В частности, это способ интеграции и конвергенции данных на основе онтологического описания, так как системы мониторинга используют огромное количество данных наблюдения (большие данные), причем данные, как правило, имеют разную структуру и могут находиться на разных серверах и в разных облачных структурах. Это приводит к необходимости разработки сервисов для решения прикладных задач в облачной среде. В связи с описанными проблемами возникает необходимость сбора и интеллектуального анализа разнородных данных, включая данные, полученные из Интернет-пространства. Наличие соответствующих метаданных становится важным условием совместного использования (свойство интероперабельности) данных в разных приложениях, в различных средствах анализа и визуализации информации о динамике информационных процессов. При размещении самоописываемых данных (метаданных) и программы внутри базы данных можно получить преимущества параллелизма, непроцедурных запросов и независимости данных, присущие традиционным системам баз данных. Следовательно, полагаться только на имена и типы параметров сервиса недостаточно. Это особенно важно для цепочек облачных сервисов. Чтобы избежать недоразумений, семантическая совместимость требует общего понимания типов переданных данных.

Одной из сложностей оценки безопасности является постоянно и значительно возрастающий агрегат информации. Это данные о сетевых и информационных ресурсах, данные о задачах, пользователях, средствах защиты, персональные данные и т.д. При этом, как правило, такая информация не имеет стандартизированного электронного представления в открытых форматах (используются всевозможные форматы, в том числе проприетарные), а уровень ее структуризации и полноты не соответствует современным критериям с точки зрения организации аналитических работ. Перечисленные особенности затрудняют формирование набора показателей оценки безопасности информационной системы.

Предлагается создание автоматизированной информационной системы для наблюдения и контроля состояния системы распределенной обработки данных. В основу системы предлагается онтологическое описание ландшафта вычислительной структуры, позволяющей классифицировать угрозы, обеспечить требуемый контроль и предоставить удобный интерфейс. Система также основывается на средствах интеллектуального анализа данных, включая большие данные, на инструментах инициализации и поддержки рекомендующей системы третьего поколения, включающих построение и реализацию математических моделей, на начальном сборе данных о субъектах и объектах информационной системы, на накоплении статистических данных об активности пользователей системы, на построении онтологии, профилей субъектов и объектов, определении атрибутов профилей и их типов.

Фёдоров В.Г., Стародубцев Ю.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ЗАДАЧА КЛАССИФИКАЦИИ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

Глобализация современных информационно-телекоммуникационных систем (ИТКС), вынужденное применение при их построении иностранного оборудования и заимствованного программного обеспечения, имеющего уязвимости, а также то, что взаимодействие органов государственной власти, безопасности, обороны и правопорядка осуществляется посредством сетей связи общего пользования (ССОП) единой сети электросвязи Российской Федерации (ЕСЭ РФ), формируют новые угрозы безопасности и обороноспособности Российской Федерации. Появился новый фактор, который снижает устойчивость ИТКС органов государственной власти - это деструктивные программные воздействия. Объектами воздействия становятся автоматизированные системы управления широкого класса назначения, причем деструктивные воздействия могут быть осуществлены из любой точки на любую точку в границах общемирового единого информационно - телекоммуникационного пространства (ОМЕИТП).

Аналитический обзор деструктивных программных воздействий на информационные ресурсы РФ показал, что имеет место ежечасное увеличение их количества и количества вскрытых уязвимостей программного обеспечения, используемых для проведения ДПВ и несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест и

локальных сетей, подключенных к ССОП.Если в 2005 году было зарегистрировано 333000 новых угроз (вирусы, черви, троянские кони и др.), то в 2014 году число таких угроз из расчета на год составило 16495000. Это означает, что каждый час создается 1883 вредоносных кода!

Средства реализации ДПВ на ИТКС представляют собой совокупность программных или программно-аппаратных средств. Цель деструктивных программных воздействий – организация канала утечки информации, блокирование, модификация, уничтожение информационных ресурсов, блокирование средств защиты информации атакуемого объекта.

Эффективная защита от потенциальных компьютерных атак невозможна без их детальной классификации, облегчающей их выявление и задачу противодействия им.

В настоящее время в различной литературе предложены классификации ДПВ, которые могут служить основой для исследования свойств и средств противодействия им. Однако известные классификации обобщают атаки для сетей общего пользования типа Интернет, не имеют классификационных признаков систематизации данных, недостаточно информативны, носят частный характер обобщения отдельных атак на конкретные операционные системы, и не являются строго научной классификацией ДПВ.Появление новых ДПВ приводит к снижению эффективности применения существующих классификаций, поэтому их использование без внесения изменений не представляется возможным. Данная ситуация объясняется огромным количеством различных сетевых атак и постоянным появлением новых атак, некоторые из которых не подчиняются критериям существующих классификаций.

В работе делается допущение, что из множества существующих ДПВ возможно выделить квазиоднородные классы угроз. Которые отличаются лишь тем, что адоптированы к микропеременным условиям воздействия, но по своей сути действуют по одному алгоритму. Поэтому данная классификация является первым шагом, позволяющим разработать методики разделения единого множества ДПВ на их устойчивое подмножество, для того чтобы существенно сократить затраты сил, средств и времени на разработку адекватных мер защиты.

Таким образом, применение существующих классификаций нельзя назвать рациональным. Существует объективная необходимость в создании новой гибкой классификационной схемы известных и возможных ДПВ, построенной с учетом указанных выше недостатков и позволяющей выработать единый подход к противодействию им.

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

УГРОЗЫ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВОЕННОЙ АКАДЕМИИ СВЯЗИ

В Военной академии связи (ВАС) сосредоточены значительные информационные ресурсы различных видов и типов, выраженных в различных формах, влияющих на ее деятельность. Значимость этих ресурсов чрезвычайно высока и поэтому существует необходимость постоянно контролировать их безопасность, то есть возрастает потребность в защите этих ресурсов как от несанкционированных действий, так и от влияния других факторов. Для обеспечения надежной защиты, необходимо постоянно держать во внимании и анализировать всевозможные источники угроз, сопоставлять им уязвимости и определять потенциальные угрозы, реализация которых прямо или косвенно может нанести вред информационной системе (ИС) Военной академии связи. Так как основой ИС Военной академии связи, является территориально распределенная локальная вычислительная сеть (ЛВС), элементы которой расположены на всех военных городках ВАС, то и угрозы безопасности будут схожи с существующими на сегодняшний день для ЛВС,но и присутствовать специфические каналы несанкционированного доступа. Это вызвано тем, что для функционирования такой территориально распределенной ЛВС требуется обеспечить высокий уровень оснащенности автоматизированной системы вычислительной техникой (автоматизированные рабочие места, сервера, сетевое и телекоммуникационное оборудование).

Основными угрозами безопасности для информационной системы ВАС являются:

- хищение (копирование информации);
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- навязывание ложной информации.

Такие угрозы безопасности ИС ВАС могут быть реализованы в связи с объединением ЛВС кафедр и удаленных абонентов в единую сеть, а так же значительной территориальной распределенности элементов ИС.

Одним из факторов появления угрозы безопасности информационной системы является размещение нескольких программных серверов на одном аппаратном, что в свою очередь вызывает необходимость представления доступа к данному серверу различных категорий пользователей. В

связи с чем у пользователей, непреднамеренные действия которых могут нанести наибольший вред ИС, появляется возможность доступа к информации, не принадлежащей им.

Таким образом, организация обеспечения информационной безопасности должна носить комплексный характер. Она должна основываться на глубоком анализе негативных всевозможных последствий. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению (уязвимостей) и как следствие определение актуальных угроз информационной безопасности.

Анализ угроз информационной безопасности является одним из ключевых моментов политики безопасности любой ИС. Разрабатывая политику безопасности, целесообразно использовать системный подход. Под системностью понимается, прежде всего то, что защита информации заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла ИС, с применением единой совокупности законодательных, организационных и технических мер, направленных на выявление, отражение и ликвидации различных видов угроз информационной безопасности.

Чеснаков М.Н., Латушко Н.А., Карпов А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ТРЕБОВАНИЯ К ОПЕРАТОРАМ СВЯЗИ ЕДИНОЙ СЕТИ ЭЛЕКТРОСВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПРЕДОСТАВЛЯЮЩИМ УСЛУГИ СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В настоящий момент сложилась ситуация, в результате которой, в системегосударственного управления используют телекоммуникационный ресурс, арендуемый у операторов связи Единой сети электросвязи Российской Федерации (ЕСЭ РФ). Однако требования, предъявляемые к операторам, в полной мере не определены, нормативно-правовая база не согласованна с потребностями спецпотребителей.

Получил некоторое распространение термин «доверенный оператор». Под этим термином понимают оператора, предоставляющего услуги системам управления органов государственной власти, четко сформулированные требования к нему отсутствуют.

В интересах обеспечения информационной безопасности необходимо провести работу по уточнению требований к операторам связи ЕСЭ РФ, с последующим закреплением этих требований в соответствующих нормативно правовых актах.

Базовые требования к операторам связи ЕСЭ РФ, предоставляющих услуги спецпотребителям:

– Обоснованное предоставление части ресурса оператора, в интересах системы государственного управления;

– Оператор должен обеспечить возможность обоснованного контроля параметров и управления телекоммуникационным оборудованием, предоставляющим ресурс системе государственного управления;

– Обеспечить возможность предоставления маршрута в соответствии с ограничениями, заданными потребителем услуг.

Описанные выше, для примера, требования должны постоянно уточняться и дополнятся с целью построения сетей со следующими свойствами:

– Временное, динамично изменяемое выделение и контролируемое использование части общего телекоммуникационного пространства для реализации совокупности процессов (технологических процедур) заданных системой управления;

– Контроль параметров (характеристик) элементов системы связи общего пользования и удержание (изменение) их в желательном состоянии.

Решение этой первоочередной задачи позволит:

– формировать логические контролируемые зоны в интересах обеспечения динамической защиты телекоммуникационных ресурсов;

– формировать сквозные (составные) каналы (тракты), соответствующие потребностям потребителя;

– обосновывать требования к перспективным средствам защиты, в том числе и коллективного использования;

– разработать унифицированные алгоритмы взаимодействия разнородных операторов и потребителей.

Шерстюк М.Ю.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»

ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ УЧЕТНЫХ ДАННЫХ В АСУС В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблеме обеспечения безопасности в современных АСУС уделяется большое внимание. В качестве средства обеспечения информационной безопасности чаще всего выступает система

мониторинга и анализа событий информационной безопасности, основными задачами которой являются:

– классификация типов событий информационной безопасности, встречающиеся в конкретной АСУС, и определение их отличительных характеристик;

– классификация типов источников и настройка средств сбора событий информационной безопасности;

– накопление и хранение событий информационной безопасности, полученных от соответствующих средств сбора;

– анализ накапливающихся событий информационной безопасности на предмет выявления инцедентов нарушения информационной безопасности в АСУС на основе набора правил, выискивающих определенные закономерности в поступлении событий, а также в значениях характеристик этих событий.

Для выполнения вышеперечисленных задач в такой системе дополнительно необходимо решать задачу учета сведений, требующихся для выполнения этих задач. В качестве таких сведений могут выступать:

– сведения о контролируемых объектах безопасности в АСУС, которые в конечном итоге могут подвергаться атакам со стороны злоумышленника;

– наиболее критичные параметры функционирования объектов безопасности, которые необходимо защищать с точки зрения информационной безопасности;

– учетные сведения по настройке элементов подсистемы сбора событий информационной безопасности по отношению к объектам безопасности в АСУС;

– события информационной безопасности, описывающие изменения значений учитываемых параметров функционирования контролируемых объектов безопасности в АСУС;

– правила автоматического поиска инцедентов нарушения информационной безопасности;

– всевозможные элементы системы отчётов по накопленным событиям и прецедентам информационной безопасности.

Разнородность учетных сведений, подлежащих хранению в таких системах, создает задачу построения информационного хранилища таким образом, чтобы обеспечить эффективность использования этих сведений для всех решаемых системой задач. При решении задачи проектирования информационного хранилища учетных сведений в общем случае должны учитываться состав и разнородность хранимых сведений, которые заставляют искать золотую середину между применением традиционного реляционного подхода с выбором уровня нормализации таблиц, а также между noSQL подходами построения информационного хранилища для документ-ориентированных категорий учётных сведений.

Необходимо учитывать, что информационное хранилище учетных сведений системы мониторинга информационной безопасности является самостоятельным объектом безопасности в АСУС, который нужно защищать от не правомерного изменения целостности и достоверности сведений учёта путём проведения ряда мероприятий, таких как:

– разрешение взаимодействия с информационным хранилищем только сервера средства обеспечения информационной безопасности на уровне аутентификации и авторизации;

– проектирование средства обеспечения информационной безопасности таким образом, чтобы не допускать выполнения команд управления информационным хранилищем посредством выполнения SQL-иньекций;

– репликация информационного хранилища на несколько оперативно обновляемых копий с целью повышения живучести информационного хранилища в случае программно-аппаратных сбоев.

ШубадеевА.С.,ЛогиновВ.А.,Кий А.В., Газин А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

СОДЕРЖАНИЕ ПЛАНИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Обеспечение защиты информации, на современном этапе развития и использования современных информационных и сетевых технологий, является одним из видов деятельности органов управления любых уровней. Деятельность по обеспечению комплексной защиты информации должна осуществляться с учетом требований соответствующих руководящих документов, регламентирующих вопросы защиты информации на объектах вычислительной техники. Мероприятия по защите информации и контроль их выполнения осуществляются на основе уточненной (разработанной) политики безопасности, а также корректного, полного и непротиворечивого плана защиты.

При планировании защиты информации необходимо учитывать: перечень защищаемых информационных ресурсов; перечень актуальных угроз защищаемой информации; условия функционирования и конфигурации объектоввычислительной техники; меры по защите информации от НСД; руководящие документы по организации защиты информации на объектах вычислительной техники.

При определении перечня защищаемых ресурсов и актуальных угроз необходимо провести анализ условий функционирования и конфигурации объектоввычислительной техники, при этом следует обращать внимание на: расположение объектоввычислительной техники; состав технических средств; организационно-штатную структуру объектоввычислительной техники; уровень профессиональной подготовки пользователей вычислительной техники.

Определенный перечень защищаемых ресурсов и актуальных угроз, в конкретной сложившейся ситуации, должен явиться основой для разработки документов по планированию защиты информации. При этом должны обеспечиваться: конфиденциальность, целостность и доступность информации.

Разрабатываемые документы должны отвечать следующим требованиям:

– обеспечивать проверку системы защиты на соответствие нормативным документам.

– обеспечивать контроль правил корректного использования средств защиты в зависимости от их состава и назначения.

– обеспечивать контроль целостности и подлинности компонентов системы защиты.

Вариант перечня вопросов отражаемых в документах планирования защиты информации может включать:

Общие положения - сведения о правовых актах, общие сведения об объекте вычислительной техники.

Обязанности должностных лиц по защите информации от НСД на объектах вычислительной техники, личного состава органа безопасности информации на объектах вычислительной техники.

– порядок организация защиты информации от НСД на объекте вычислительной техники–план выполнения всех мероприятий по защите информации.

– порядок организация защиты информации от воздействия вирусов.

– порядок учета, хранения носителей информации, а также документов и обращение с ними.

– контроль за организацией и состоянием работы по защите информации от НСД на объекте вычислительной техники.

– действия личного состава в случаях НСДк информации, стихийного бедствия, техногенных катастроф.

Шустров Е.С., Шустрова Е.Ю., Иванцов Е.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Москва, в/ч 52686

ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМОВ УПРАВЛЕНИЯ МАРШРУТИЗАЦИЕЙ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

В настоящее время идет качественный перевод системы управления Вооруженных Сил Российской Федерации на новый уровень. Это оснащение стационарной и полевой компоненты системы связи цифровым телекоммуникационным оборудованием, подготовка и переподготовка необходимых кадров. Построение общего инфокоммуникационного пространства для функционирования и предоставления доступа к услугам связи должностных лиц различных звеньев управления, видов Вооруженных Сил и родов войск.

Применение новых перспективных образцов средств связи, которые имеют более высокие тактико-технические характеристики, расширяют, тем самым, возможности и в то же время уязвимости системы связи. Возрастают требования, предъявляемые к ней и к ее построению, комплектованию, профессиональной выучке личного состава аппаратных связи и пользователей коммуникационных услуг.

Возникает вопрос о реализации оптимизации маршрутизации в системе межвидовой и межуровневой сети передачи данных, то есть, решение задачи оптимального распределения потоков данных между элементами сети передачи данных. Повышается устойчивость системы передачи данных, нагрузка на узлы коммутации распределяется равномерно.

Оптимизация маршрутизации в сети передачи данных можно реализовать путем поиска функции распределения потоков, которая описывается различными показателями. Данные показатели имеют определенные диапазоны, которые формируют у функции распределение потоков некоторую область значений.

Так как состав, структура и связность системы связи объединения определены, то можно сказать что, для данной структуры оптимальны будут маршруты доставки пакетов различных потоков, в определенной области значений функции распределения, которые в свою очередь достигаются путем нахождения показателей этой функции в оптимальных диапазонах значений.

Для реализации этого вопроса необходимо определить набор этих показателей и наиболее подходящийдиапазон значений, которые будут отвечать требованиям оптимальности, предъявляемые для данной структуры и связности.

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

АЛГОРИТМ ЦЕНТРАЛИЗОВАННОГО ЦЕЛЕРАСПРЕДЕЛЕНИЯ В СИСТЕМАХ РАДИОПОДАВЛЕНИЯ

Функционирование систем управления в условиях конфликта характеризуется активным воздействием противоборствующих сторон друг на друга с целью достижения информационного превосходства. Одним из путей достижения которого является активное воздействие на систему связи противника. Помимо физического уничтожения элементов системы связи, активно применяются методы радиоэлектронного воздействия. Анализ показывает, что условия функционирования систем управления и связи и системы воздействия взаимосвязаны. Это даёт возможность на основании прогноза функционирования системы воздействия обосновать направления защиты системы связи в условиях информационного противоборства.

Одним из элементов системы связи являются сети радиосвязи (СРС) функционирующие в условиях преднамеренных помех, постановку которых осуществляет система радиоподавления (СРП) противоборствующей стороны. В СРП входит подсистема целераспределения и передатчики помех. Система целераспределения может функционировать по централизованному или децентрализованному алгоритму. Централизованное целераспределение означает, что частотный ресурс всех передатчиков помех распределяется между обнаруженными всеми приемниками радиоразведки.

Целераспределение это процесс «назначения» частот передатчикам помех комплексов радиоподавления (КРП), проводимый по результатам цикла разведки с учетом ограничений на частотный ресурс ПП. В комплексах РП информация от всех приемников разведки поступает на централизованный пункт управления, в котором производится ее интегрированная обработка. Именно такой вариант централизованной обработки информации используется в данной задаче целераспределения.

Задачей целераспределения является определение условных номеров РЭС, подлежащих радиоэлектронному подавлению, и распределение этих объектов по средствам РП, входящим в КРП. Причем эффект, производимый РП, должен быть максимальным по влиянию на своевременность и достоверность передачи информации в СРС.

Задача решается методом комбинаторной оптимизации. Физический смысл нахождения рационального варианта назначения частот для РП заключается в том, что каждое РЭС СРС будет подавляться именно тем средством РП, уровень помехи от которого будет максимальным. Для решения данной задачи предлагается эвристический алгоритм, приводящий к рациональному решению за конечное число шагов.

Решение задачи позволяет системе целераспределения предоставлять данные лицу принимающему решение (оператору) для эффективного использования средства РП. А при организации защиты системы связи, прогнозировать «поведение» СРП с целью реализации дифференцированного подхода к противодействию радиоподавлению.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Алексанков С.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МОДЕЛЬ ДИНАМИЧЕСКОЙ МИГРАЦИИ ВИРТУАЛЬНЫХ МАШИН

Высокая надежность, отказоустойчивость и безопасность систем критического применения, в частности, функционирующих в реальном времени, реализуется при резервировании основных подсистем, в том числе средств хранения, обработки и передачи данных.

Для обеспечения непрерывности доступа клиентов к приложениям и сервисам используются кластеры высокой доступности. Высокая доступность ресурсов кластерной системы в случае сбоя одного из серверов или при проведении профилактических работ обеспечивается за счет перемещения служб или приложений между узлами. Для клиента кластер выглядит как единое целое и его неполадки могут выразиться в кратковременном снижении производительности или недоступности какого-либо ресурса на время от нескольких секунд до нескольких минут в зависимости от конфигурации.

Миграция виртуальных машин является важной возможностью технологии виртуализации, которая позволяет приложениям прозрачно перемещаться вместе с их средами выполнения между физическими машинами. Динамическая миграция («Live Migration») позволяет переносить виртуальные машины практически без прерывания выполнения приложений. Это новая технология включена в пакеты самых популярных систем виртуализации (Microsoft HyperV, VMvare VSphere, Xen). Динамическая миграция характеризуется тем, что работа виртуальных машин не останавливается при переносе.

В общем, процесс динамической миграции можно разделить на два шага – 1) передача управления узлу назначения, 2) передача данных (память, диск) на узел назначения. Существуют два наиболее распространенных подхода к реализации динамической миграции, основанные на различной последовательности этих шагов:

– с копированием до остановки: сначала происходит передача данных, а затем – передача управления;

– с копированием после остановки: сначала происходит передача управления узлу назначения, а затем – передача данных;

В данной работе рассматривается второй подход (с копированием после остановки или т.н. подход с копированием в фоновом режиме). Цель работы – разработка модели динамической миграции виртуальных машин с с копированием после остановки, с помощью которой можно оценить время недоступности сервисов при переносе виртуальных машин при различных параметрах, таких как интенсивность приложения изменения памяти, интенсивность перемещения страниц памяти, объем образа памяти виртуальной машины.

Аминов Х.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКАХ

В связи с активным развитием банковских информационных систем и технологий, вопросы обеспечения информационной безопасности в банках становятся особо значимыми и актуальными.

Обеспечение информационной безопасности в банках - это непрерывный процесс, который состоит из различных составляющих организационногои технического характера.

Общеизвестно, что банки оперируют денежными средствами, предоставляют своим клиентам большое количество сервисов и хранят персональные данные клиентов - физических лиц и конфиденциальную информацию клиентов – юридических лиц. Незаконное манипулирование и утечка такой информации может привести к серьезным убыткам. Отсюдаследует, что вопросы информационной безопасности занимают важное место в деятельности банков и к ним предъявляются жесткие требования.

В настоящих условиях для успешного функционирования, банкам необходимо организовать систему управления информационной безопасности в соответствии с требованиями многочисленных законодательных актов и стандартов. В области информационной безопасности в мире

насчитывается около 600 стандартов. В России в качестве основных выделяют две группы стандартов: международный стандарт ИСО/МЭК 27001 и комплекс стандартов Банка России СТО БР ИББС. Данные стандарты регламентируют вопросы создания, внедрения и эксплуатации системы управления информационной безопасности в различных типах организаций.

Большое внимание в данных стандартах уделяется вопросам наличия и доступности информации, документов и технических средств, необходимых для функционирования банков. Специфику банковской сферы России больше учитывает стандарт Банка России, и оно рекомендуется к применению в банках. Комплекс стандартов Банка России СТО БР ИББС постоянно обновляются по результатам их применения и изменений в законодательстве. Кроме этого, Банком России разработаны и введены рекомендации в области стандартизации информационной безопасности, которые также имеют практическую значимость.

Необходимость обеспечения информационной безопасности связано с возникновением различных видов угроз. Сегодня банки и их клиенты могут столкнуться с многочисленными угрозами (например, DDOS-атаки, вирусы, спам и др.).

В последнее время наблюдается рост количества атак на системы интернет-банкинга. Данные угрозы во многом связаны с извлечением финансовой выгоды. С целью предотвращения угроз, необходимо и дальше разрабатывать и внедрять организационные решения, технические и программные средства защиты информации. Следует отметить, что обеспечение информационной безопасности охватывает не только защиту информации в компьютерных сетях, но и защиту информации на других носителях и интеллектуального капитала сотрудников банка.

По данным Банка России, 80% всех проблем в области информационной безопасности решаются административными, организационными и процедурными средствами и только 20% проблем могут быть решены техническими и программными средствами (антивирусы, криптографическая защита, протокол SSLи др.). Отсюда следует, что банкам, в первую очередь, необходимо организовать систему управления информационной безопасности.

Наравне с появлением новых средств и технологий, появляются новые виды угроз, следовательно, правильно организованная система управления информационной безопасности может снизить вероятность их появления и уменьшить стоимость возможного ущерба.

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

ПРОБЛЕМЫ БЕЗОПАСНОСТИ СЕТИ IP-ТЕЛЕФОНИИ ДЛЯ НАУЧНО-ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ

Доклад посвящен изучению проблем безопасности при построении сети IP-телефонии между двумя площадками научно-производственного предприятия, расположенными в разных городах. Рассматриваются возможности защиты при помощи зашифрованного VPN канала. Оценены объемы дополнительных средств, которые нужно вложить в планирование и обеспечение сетевой безопасности.

В докладе показано, что эффективными меры безопасности могут быть только тогда, когда они покрывают все уровни сетевой инфраструктуры.

Безрук Г.Г., Левкин И.М.
Россия, Санкт-Петербург, НИИО МРТ ФГБУ ГНИИЦРТ МО РФ, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОБОБЩЕННЫЕ КОМПЛЕКСНЫЕ ПАРАМЕТРЫ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

При оценке безопасности функционирования информационных систем возникает необходимость их формализованного описания. В основу этого описания могут быть положены обобщенные комплексные параметры процесса функционирования информационной системы в составе:

– комплекса средств автоматизации (КСА) объединенных в технические средства информационного контура, непосредственно осуществляющие обработку информации;
– информационно-управляющего комплекса;
– системы обеспечения безопасности.

К обобщенным комплексным параметрам информационной системы можно отнести:

– обобщенный параметр информационного контура;
– параметры, характеризующие АРМ специалиста;
– параметры, обусловливающие возможности системы обеспечения процесса функционирования АРМ специалиста;
– параметры объектовой обстановки;

– характеристики условий ведения мониторинга (размеры области поиска), свойства объектов и т.п.);

– параметры, характеризующие противодействие;

– обобщенные параметры средств добывания информации (приемно-измерительных комплексов): оперативность, полнота и точность добываемой информации, физическая сущность принимаемых сигналов, степень семантической доступности к ним и др.;

– обобщенные параметры информационных органов;

Характеристики системы обеспечения отображаются векторами:

– технического обеспечения;
– математического обеспечения;
– программного обеспечения;
– информационного обеспечения;
– организационного обеспечения;
– правового обеспечения.

Анализ этих обобщенных комплексных параметров свидетельствует, что условия любого нового проекта случайным образом влияют практически на все характеристики векторов (за исключением характеристик вектора) и целевой функции.

Декомпозиция системы информационной безопасности в рамках иерархического подхода позволяет представить ее основные составные части в виде соответствующих операционных комплексов. Параметры операционного комплекса также связаны с обобщенными комплексными параметрами информационной системы.

Несмотря на это, сформулировать общий показатель эффективности всей системы информационной безопасности не представляется возможным в силу большого числа информационных узлов и их иерархической структуры.

Поэтому для оценивания эффективности системы информационной безопасности разработана методика, состоящая из трех уровней, позволяющая рассчитывать эффективность процесса решения задач информационной безопасности - вычислять математическое ожидание и дисперсию числа решенных системой задач.

Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОПТИМИЗАЦИЯ СТРУКТУРЫ И ПРОЦЕССА ПЕРЕРАСПРЕДЕЛЕНИЯ ЗАПРОСОВ В МУЛЬТИКЛАСТЕРНЫХ СИСТЕМАХ

Обеспечение экономической безопасности организаций предполагает отказоустойчивость корпоративной инфокоммуникационной системы, в том числе отказоустойчивость и высокую доступность центров обработки и хранения данных.

Отказоустойчивость и высокая доступность центров хранения и обработки данных достигаются при консолидации ресурсов в результате их объединения в кластеры, в которых реализуется динамическое перераспределениезаданий с учетом деградации при накоплении отказов и проявлений деструктивных воздействий.

В настоящее время актуальность оптимизации перераспределения запросов возрастает в связи с возникновением мультикластерных систем и интенсивным развитием распределенных вычислений на основе концепции Грид (GRID) - распределенной инфраструктуры, объединяющей множество ресурсов, доступных из любой точки, независимо от места их расположения, в том числе относящихся к различным кластерам.

Таким образом, отказоустойчивость современных инфокоммуникационных систем может обеспечиваться при консолидации распределенных ресурсов мультикластерных систем.

При проектировании распределенных мультикластерных систем ставится задача оптимизации структуры системы и процесса распределения потока запросов между кластерами.

Задача оптимизация структуры является статической (выполняется до начала функционирования системы), а задача распределения запросов может быть динамической, выполняемой в процессе функционирования системы на основе мониторинга и измерения текущего состояния загруженности узлов системы и характеристик потока запросов.

При оптимизации структуры, требуется для заданных ограничений на стоимость реализации системы найти число (кратность резервирования) коммутационных узлов, а также число серверов в локальных кластерах обеспечивающих наибольшую надежность системы и наименьшее время пребывания в ней запросов.

В результате оптимизации процесса распределения потока запросов, поступающего в некоторый кластер, ищется их доля, выполняемая с использованием ресурсов данного кластера и доля запросов, перераспределяемая через сеть в другие кластеры.

Известные модели мультикластерных систем в качестве основного показателя качества обслуживания ориентированы на среднее время пребывания запросов, что ограничивает их использование при проектировании систем реального времени, эффективность которых оценивается по вероятности не превышения допустимого времени ожидания запросов в очереди.

В направлении совершенствования методологии автоматизированного оптимального проектирования мультикластерных систем, в том числе проектирования мультикластерных систем реального времени, ставится задачи разработки:

– модели массового обслуживания мультикластерных систем, для оценки среднего времени пребывания запросов, вероятности своевременности и безошибочности обслуживания запросов с учетом возможности их взаимного перераспределения через сеть между кластерами в условиях накопления отказов узлов и их временных отключений, а также изменяющейся интенсивности потока запросов;

–методов оптимального проектирования структуры мультикластерных систем и процесса взаимного перераспределения запросов между кластерами, с целью консолидации ресурсов при минимизации среднего времени ожидания, а для систем реального времени с целью максимизации вероятности своевременного и безошибочного обслуживания запросов, в условиях адаптации к отказам, ошибкам и временным отключениям узлов.

Богатырев В.А., Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИОННЫХ УСЛУГРЕАЛЬНОГО ВРЕМЕНИ В УСЛОВИЯХ ОШИБОК, ОТКАЗОВ И ДИСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Повышение готовности (доступности), безотказности и отказоустойчивости информационных систем традиционно достигается в результате резервирования узлов хранения обработки и передачи данных. Резервирование вместе с тем приводит к удорожанию системы, и к росту энергопотребления, что влечет дополнительные эксплуатационные потери и снижение экономической эффективности предоставления информационных услуг. При построении кластерных систем предоставления информационных услуг реального времени, когда стоимость услуги зависит от своевременности обслуживания запросов, задержки предоставления услуги и энергопотребление кластера должны быть минимизированы.

Для обеспечения своевременности предоставления информационных услуг в зависимости от интенсивности потока запросов может потребоваться различное число активных компьютерных узлов, что позволяет реализовать режим энергосбережения на основе адаптивной реконфигурации системы, при которой часть узлов, сверх минимально необходимого числа для качественного современного обслуживания запросов, может отключаться (переключаться в холодный резерв). При обнаружении увеличения потока запросов происходит адаптивное подключение необходимого числа узлов, находящихся в холодном резерве. В случае же снижения нагрузки часть активных узлов переключается в холодный резерв. Исследуемая организация адаптивной энергосберегающей реконфигурации кластерных систем позволяет обеспечить ее адаптацию не только к отказам узлов, и изменениям потоков запросов пользователей, но и определенную устойчивость к деструктивным воздействиям не только случайного, но и злонамеренного характера, в том числе к угрозам DDOS-атак.

Для повышения устойчивости к отказам и ошибкам вычислительного процесса в кластерных х системах реального времени копии запросов могут распределяться на выполнение в несколько узлов кластера, чем достигается резервирование вычислительного процесса.

В кластерных системах, узлы которых представимы одноканальными системами массового обслуживания с локальными очередями, возможна существенная разница времен ожидания в очередях, что потенциально может привести к увеличению вероятности выполнения резервированных запросов к требуемому времени хотя бы в одном узле кластера, несмотря на влияние резервирования запросов на увеличения нагрузки узлов.

Представляется актуальным исследование возможностей адаптивной энергосберегающей реконфигурации кластерных систем, которая потенциально может привести к повышению экономической эффективность предоставления информационных услуг в реальном времени.

В кластер с интенсивностью Λ поступает общий поток запросов, каждый из которых может быть принят или не принят к обслуживанию. В случае отказа предоставлении услуги по запросу будем считать, что штраф или какие либо иные санкции не налагаются. В случае же принятия запроса к обслуживанию и не предоставления безошибочных результатов в заданные сроки - налагается штраф.

Принятые к обслуживанию запросы распределяются в очереди одного из узлов, или в случае их критичности в (критичность может определяться значительностью санкций за невыполнение, несвоевременное или ошибочное выполнение запроса) копии запроса могут направляться в очереди нескольких узлов.

Будем полагать, что при предоставлении информационных услуг в реальном времени, прибыль от безошибочного выполнения каждого запроса, если время его ожидания была меньше t0 равна a1, а если больше t0 или результат ошибочный, то налагается штраф равный a2, при этом расходы на электропитание каждого узла в единицу времени равны a3.

Целью работы является исследование возможностей повышение экономической эффективности предоставления информационных услуг в реальном времени в результате адаптивной энергосберегающей реконфигурации системы, сопровождающейся отключением компьютерных узлов, избыточных для обеспечения требуемого качества и своевременности услуг. При этом предложены модели кластера, позволяющей оценить эффективность предоставления информационных услуг реального времени в зависимости от интенсивности входного потока запросов, отказавших узлов и узлов, переключаемых в холодный резерв, в том числе с учетом возможности резервного обслуживания запросов.

Богатырев В.А., Паршутина С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МОДЕЛИ МНОГОПУТЕВОЙ ОТКАЗОУСТОЙЧИВОЙ МАРШРУТИЗАЦИИ

Надежность хранения, передачи и обработки данных, особенно в системах критического применения важнейших отраслей народного хозяйства, таких как топливно-энергетический комплекс, транспорт, связь и другие, определяет устойчивое развитие и информационно-экономическую безопасность системы.

Целью исследования является повышение надежности и сокращение задержек распределения запросов через сеть на основе многопутевой маршрутизации.

Рассматриваются варианты организации распределения запросов через сеть при последовательном и параллельном обращении к узлам – потенциальным приемникам запросов (серверам) и строятся модели таких вариантов распределения запросов. При построении моделей необходимо учитывать, что одновременная передача запросов по нескольким маршрутам приводит к росту нагрузки в сети, причем она дополнительно увеличивается из-за формирования потока возвращенных (повторных) запросов при обращении к отказавшим или недоступным для обслуживания запросов серверам. Сравнение вариантов распределения запросов проводится по среднему времени их задержки в сети.

Предлагаются модели распределенных вычислительных систем при многопутевом перераспределение запросов через сеть с динамическим выбором маршрута. Рассмотрены варианты распределения запросов, когда узел-источник запроса отсылает его (запрос) узлу-приемнику по одному пути и когда передача запроса резервируется и осуществляется по нескольким маршрутам одновременно. Если передача не удалась, запрос пересылается через сеть повторно, но уже по другому маршруту (маршрутам), и так до тех пор, пока породивший запрос узел не получит подтверждение о его успешной пересылке.

В простейшем случае пути не пересекаются, а выбор маршрута задается случайным или циклическим образом. Каждый маршрут представляется одноканальной системой массового обслуживания типа M/M/1 с бесконечной очередью при бесприоритетной дисциплине обслуживания. Сравнение вариантов распределения запросов проводится по среднему времени задержки запросов в сети.

Время пребывания запроса и вероятность успешной доставки информации за требуемое время в сети в условиях сбоев, отказов и деструктивных воздействий определяется, в первую очередь:

– интенсивностью сбоев и отказов и деструктивных воздействий;

– интенсивностью потока запросов с учетом первоначальных и повторных обращений к принимающим запросы серверам;

– готовность серверов к приему и выполнению запросов в условиях возможных отказов, отключений и временной недоступности серверов для обслуживания поступающих через сеть запросов;

– кратность резервирования, или число маршрутов, задействованных для одновременной пересылки запроса через сеть.

При анализе полученных моделей установлено, что резервирование передачи запросов по сети целесообразно при низкой готовности серверов-приемников запросов, тогда как при их высокой готовности эффективней распределять запросы через сеть по одному пути.

Богатырев В.А., Паршутина С.А., Попцова Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МНОГОПУТЕВАЯ ОТКАЗОУСТОЙЧИВАЯ МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ И ГИБРИДНЫХ СЕТЯХ С РЕЗЕРВИРОВАННОЙ ПЕРЕДАЧЕЙ ДАННЫХ

Экономическая эффективность и безопасность информационных систем предприятия определяются его информационной инфраструктурой и способами ее поддержания и развития. Особое место в этой связи отводится процессам передачи и обработки данных, в частности организации эффективной маршрутизации на базе существующего сетевого оборудования.

Многопутевая маршрутизация призвана решить проблему балансировки нагрузки в сети в рамках доступной пропускной способности каналов и обеспечить надежную передачу данных в условиях отказов и перегруженности запросами узлов сети и линий связи, а также – в случае беспроводных сетей – ошибок, возникающих из-за ненадежности среды передачи, потери питания отдельными узлами и т.п.

Особый исследовательский интерес представляют гибридные вычислительные сети, которые сочетают в себе достоинства проводных сетей, такие как энергонезависимость отдельных узлов и устойчивость к электромагнитным помехам в среде передачи, и беспроводных сетей, в первую очередь, скорость и простоту их развертывания, особенно на местности, где прокладка кабеля затруднена.

Цель исследования заключается в повышении надежности и отказоустойчивости беспроводных и гибридных вычислительных сетей, уменьшении задержек в сети при адаптивном распределении запросов на основе многопутевой маршрутизации.

Предполагается построение и анализ моделей распределения запросов через сеть при опросе одного или одновременно нескольких серверов, принимающих поступающие из сети запросы. В случае успешного распределения запроса узел-источник получает уведомление о его доставке, в противном случае запрос посылается по другим маршрутам. Выбор каждого следующего пути определяется на основе некоторого алгоритма, например, кругового обслуживания (Round-Robin).

В качестве критерия эффективности распределения запросов через сеть выбрано среднее время задержки в сети – среднее время доставки запросов на узел-приемник с учетом повторной пересылки.

Передача запроса одновременно по многим маршрутам повышает вероятность его доставки хотя бы на один сервер-приемник при каждой пересылке, особенно в условиях высокой интенсивности отказов оборудования на узлах, помех в линиях связи и ошибок маршрутизации в результате динамической перестройки топологии сети – как в беспроводных сетях, состоящих из мобильных устройств (MANET). В то же самое время параллельное распределение запросов через сеть и их повторная передача при неуспешной доставке, увеличивает интенсивность потока запросов и может привести к перегрузке в сети.

Представляется актуальной задача вычисления кратности резервирования, или нахождения оптимального числа маршрутов при одновременном распределении запросов через сеть, для беспроводных и гибридных вычислительных сетей. Показано, что резервирование маршрутов целесообразно при невысокой готовности серверов к приему запросов из сети, в то время как при высокой готовности серверов-приемников параллельная пересылка запросов приводит к увеличению среднего времени задержки.

Богатырев В.А., Сластихин И.А.
Россия, Санкт-Петербург,Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МОДЕЛЬ РЕЗЕРВИРОВАННОГО ОБСЛУЖИВАНИЯ ЗАПРОСОВ В МНОГОКАНАЛЬНЫХ СИСТЕМАХ

Доклад посвящен разработке многоканальной модели обслуживания с оценкой экономической эффективности предоставления информационных услуг при резервированном обслуживании запросов.

Выбор организации вычислительного процесса по обслуживанию запросов в системах информационного сервиса во многом определяется экономической эффективностью своевременного и безошибочного предоставления информационных услуг.

Эффективность систем информационного сервиса охарактеризуем прибылью от безошибочного и своевременного предоставления информационных услуг, получаемую в единицу времени. Будем предполагать, что прибыль от предоставления услуг зависит от задержкиих обслуживания и при этом существует пороговое значение задержки,связанная со штрафными санкциями.

Для анализа задержек рассматриваемую информационную систему представим в виде многоканальной системы массового обслуживания с бесконечной общей очередью запросов. Предполагается, что входящий поток является простейшим, а обслуживание - экспоненциальным. При выполнении запроса возможны отказы и ошибки. Будем считать вероятность правильного выполнения запросов одинаковой для всех каналов. Для критических запросов (задержка выполнения которых связана с существенными штрафными санкциями) предусматривается резервированное выполнение копий запроса в нескольких каналах. При резервированном обслуживании запрос считается выполненным, если верно выполнена хотя бы одна из его копий.

Показано, что для многоканальных систем обслуживания, функционирующих в условиях отказов и ошибок, существует область эффективности резервированного обслуживания запросов. Показано, что в зависимости от интенсивности ошибок существует порог интенсивности потока запросов, выше которого резервированное обслуживание запросов становится нецелесообразным.

Показано, что увеличение эффективности предоставления информационных услуг возможно при адаптивном изменении кратности резервирования запросов в зависимости от интенсивности потока запросов и ошибок.

Бойченко О.В., Адарчина С.О.
Россия, Симферополь, Крымский институт экономики и управления
Крымского федерального университета имени В. И. Вернадского

ПРОБЛЕМА ЗАЩИТЫ МАРКЕТИНГОВОЙ ИНФОРМАЦИИ САЙТОВ

Актуальность исследования обусловлена достаточно высокой степенью простоты доступа к коммерческим данным сайта компании, необходимым для интернет-маркетинга. Это обуславливает проведение научных исследований по проблематике несанкционированного доступа к коммерческой информации сайтов без привлечения активных способов получения данных (размещение вирусных кодов, ddos-атаки, несанкционированный доступ и прочее).

Такая ситуация создает условия для скрытого (неочевидного) доступа к данным сайта, при чем уровень нанесения ущерба становится сайту конкурента становится довольно значительным.

Практическое исследование отдельных сервисов, использующихся для анализа конкурентской базы маркетинговых данных сайта с целью продвижения аналогичного продукта или услуги, без обмана в работе с клиентами, и получением такого же капитала указывает на широкие возможности относительно доступа к коммерческой информации.

Так, сервис для анализа контекстных кампаний и поискового продвижения конкурентов SpyWords.ru обеспечивает выдачу по запросу в считанные секунды следующей информации:

- все рекламные объявления;
- ключевые слова, по которым данный рекламодатель размещает контекстную рекламу;
- позиция в поиске данного объявления;
- бюджет, выделенный на рекламу;
- трафик посетителей сайта — количество человек, заходящих на сайт;
- сравнение с конкурентами.

Анализ предоставленных данных позволяет конкуренту получить необходимую коммерческую информацию о бюджете, ключевых словах, наиболее часто используемых в запросах клиентов, эффективности расходования бюджета на рекламу, поступлениях трафика его посетителей. Полученные данные позволяют повысить конкурентоспособность сайта-клона за счет более выгодного размещения рекламного объявления и привлечения большего количества клиентов.

Исследование возможностей сервиса Publer.wildo.ru по предоставлению необходимых данных для мониторинга рекламных постов и тизеров ВКонтакте, в ОК, ТаргетМайл конкурентов, указывают на эффективность использования этого инструмента для привлечения трафика из социальных сетей, поскольку с помощью него можно получить следующую информацию:

- данные о выгодности покупки рекламы в определеннойконтактной группе;
- данные о текущих трендах в рекламе;
- данные о наибольшем спросе на товар;
- данные о способах и месте размещения рекламы конкурентов (все их посты, тизеры и т.д.).

Следует отметить, что подобных сервисов, предоставляющих как платные, так и бесплатные услуги, в Интернете достаточно большое количество. В основном они работают на базе данных с Яндекс.Директа и различных сайтов, предоставляющих рекламные услуги и SEO-оптимизацию.

Такие сервисы анализ конкурентов сайта необходимы для того, чтобы сократить время и материальные затраты на продвижение конкретной страницы сайта в ТОП поисковой выдачи. Кроме того, такой анализ позволить получить необходимую информацию о способах и инструментах продвижения, а также о возможности занять их место в поиске.

Однако, в указанной ситуации возникает острая необходимость владельца сайта по решению проблемы защиты коммерческой информации, связанной с планированием бюджета на создание

рекламы, уникального контента, дизайна, разработкой оптимальных вариантов для повышения продаж своей компании и т.д.

Это обусловлено тем, что информация о рекламе, как элемента SEO-оптимизации и интернет-маркетинга сайта, является достаточно уязвимой по причине того, что сайт изначально предназначен для публикации, то есть является открытым во всеобщем доступе, а способов и методов по противодействию несанкционированному мониторингу сайтов конкурентами в настоящее время не существует.

В заключении следует отметить, что в настоящее время существует острая необходимость создания системы методов и способов эффективного противодействия мониторингу сайтов конкурентами для защиты коммерческой рекламной информации о своём продвижении сайта и способах эффективного привлечения клиентов с помощью Интернет-технологий, а также сохранении необходимых условий для читабельности браузерами клиентов.

Васькова А.В., Михайличенко Е.М.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации

ТРАНСПОРТНЫЙ ФАКТОР КАК ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Транспорт зачастую называют внутренней «кровеносной» системой страны, а так же ее экономики, которая обеспечивает взаимодействие абсолютно всех субъектов хозяйственного комплекса. Транспорт прежде всего помогает населению удовлетворять потребности в перевозках как на дальнее расстояние, так и на местном уровне грузов, также транспорт является помощником при объединении регионовв страны. Транспортная сеть является звеном, которое связывает производителей и потребителей продукции,товаров, услуг, без которых невозможносуществование рынка и рыночные отношения. Главное социально-экономическое значение,прежде всего, для государства и общества,как раз, и состоит в этом. Поэтому огромные нарушения в работе транспортной сети повлекут за собой серьезные, глобальные последствия для экономической безопасности страны.[6]

Транспортный комплекс - это крупная сфера многоотраслевого комплекса, которая включает в себябольшой спектр видов грузового и пассажирского транспорта, к примеру, железнодорожный, автомобильный, морской, речной, трубопроводный, воздушный, промышленный и городской. Удельный вес работников, которые непосредственно связывают свою трудовую деятельность с транспортом более 4 млн.человек, а удельный вес транспорта в валовом внутреннем продуктестранына 1 января 2014 г. составил 8%.Доля транспортных расходов в совокупной стоимости всей произведенной продукции в промышленном секторе и секторе сельского хозяйства составляет около 15-20%, а по некоторым перевозкам, с учетом региональных особенностей данная доля доходит до 45-50%.

Железнодорожный транспорт Российской Федерации–это ведущая часть транспортного сектора экономики страны, которая имеетведущее значение для хозяйственных связей и платежеспособностиграждан.[2]

Железные дороги в процентном соотношениидля системы транспорта общего пользованиясоставляет 43,2 %. Доля железнодорожного транспорта, из общего объема пассажирооборота, занимает около 28,6%. Транспорт выполняет роль одного из главных стабилизаторов социально-экономического положения граждан в стране, по средствам обеспечениякрупномасштабных пассажирских перевозок при четко установленном уровне тарифов, с убыточностью до 50-60%.

Железнодорожный транспорт обеспечивает устойчивое развитие материального производства, быстрое увеличение эффективногорасходования ресурсов, эффективное сокращение себестоимости продукции при уменьшении транспортногобремя, обильный рост активности, а так же способствует быстрому решению других социальных задач. При этом из-за нехватки развития транспортных связей существуютбольшие потери в народном секторе. Железнодорожный вид транспорта в условиях развития современной России нельзя считать конкурирующим с автомобильным видом транспорта во внутригосударственных перевозках.

Самое большое количество смертейприходилось на 2012 год. В течении трех лет данные показателя сократились, и уже в 2014 году число погибших на 10 тысяч транспортных средств составляло 4,84 человек, что значительно меньше по отношению к 2012 году.

Основные угрозы экономической безопасности в транспортной сфере:

а) в сфере перевозок обуславливается:

– сокращение уровня безопасности перевозочного процесса, который определяется низким уровнем надежности используемой техники;

– наиболее высокий физический и моральным износом технической базы,в результате низких темпов ее обновления и сокращения инвестиционной активности;

– сокращением эффективной организации и управления процессом перевозки,вследствиенеэффективного применения элементов нового оборудования, а так же современного научно-технического прогресса.

б) в социальной сфере определяется:

– постоянно прогрессирующим несоответствием в заработной платев транспортной сфере и в базовых отраслях, что приводит к высокому уровню текучести кадров;

– недостаточным стимулированиемработников для получения максимального результата, в частности это соотношение между ростом производительности труда и ростом заработной платы;

– неоправданнойразницей между заработными оплаты отдельных категорий работников.

в) в финансовой сфере показывает на:

– убыточность пассажирских перевозок;

– непонятный рост инфляции, при ограничении уровня тарифов на перевозки грузов и пассажиров;

–сокращение государственной помощи в реализации инвестиционных проектов, а так же развития транспорта.

Верзун Н.А., Колбанёв М.О., Михайлов С.В.
Россия, Санкт-Петербург, Международный банковский институт

ТЕХНОЛОГИЧЕСКИЕ ОСНОВАНИЯ ПЕРИОДИЗАЦИИ ИСТОРИИ

Доклад посвящен анализу подходов к периодизации истории человечества, в основе которых лежат уровни развития материальной и информационной технологий, а также проблемы безопасности, связанные с использованием новых технологий в предметной деятельности людей.

Показано, что в новейшей истории уровень развития цивилизации определяется уровнем информатизации общества. С 90-х гг прошлого века в соответствие с теорией экономических циклов Н.Д. Кондратьева развитие мировой экономики может быть описано новой 5-й большой волной, связанной с революционными открытиями в области инфокоммуникаций. Инфокоммуникационные технологии стоят в одном ряду с технологиями глобализации, которые человечество использовало в предыдущие века. Это технологии эпох Великого шелкового пути и Великих географических открытий.

Сегодня основные направления развития информационной отрасли связаны с созданием третьей платформы информатизации, которая должна придти на смену традиционному интернету. Сеть персональных компьютеров превращается, по терминологии Cisco, в интернет всего.

Третья платформа создается за счет движения технологий в трех направлениях:

1. распределение информационных источников (умных вещей, сенсоров и др.) в реальном жизненном пространстве для автоматического сбора данных на больших территориях;

2. построение сверхмощных централизованных облачных инфокоммуникационных систем обработки этих данных;

3. увеличение скоростей мобильного доступа к инфокоммуникационным ресурсам.

Главные проблемы, возникающие на этом пути, – это безопасность, стандартизация и ресурсоемкость технологий.

Верзун Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ТЕХНОЛОГИИ БЕЗОПАСНОГО ДОСТУПА В БЕСПРОВОДНЫХ СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

Интернет вещей (InternetofThings, IoT) по определению аналитиков IDC (InternationalDataCorporation) проводная или беспроводная сеть уникальных, адресуемых конечных точек (умных вещей), имеющих автономное обеспечение, которые взаимодействуют по стандартным протоколам между собой без участия человека, управляются интеллектуальными системами, могут подключаться к Интернету, исполнять собственные или облачные приложения и анализировать собираемые данные. Также они могут обладать способностью захватывать, анализировать, передавать и принимать данные от других систем.

Технология IoT находит свое применение во многих сферах человеческой деятельности, выделяют два основных направления её использования:

– мониторинг и управление устройствами, каждое из которых может взаимодействовать с различными объектами инфраструктуры и физической среды. Например, в жилищно-коммунальном хозяйстве мониторинг расхода электроэнергии, управление системами жизнеобеспечения дома или квартиры.

– сбор данных с конечных узлов для дальнейшего их анализа с целью выявления тенденций и взаимосвязей. Например, в медицине наблюдение и анализ состояния больного.

Интернет вещей базируется на трех технологиях: идентификации, позволяющей отличить конкретную вещь от любой другой вещи; миниатюрных источниках питания и технологии передачи данных между вещами. В связи с тем, что количество умных вещей, подключенных к сети постоянно растет (так, согласно расчётам консалтингового подразделения компании Cisco IBSG, уже к 2020 году

число подобных устройств достигнет 40 миллиардов) целесообразно для передачи данных между ними использовать беспроводные технологии, которые всегда представляли интерес для создателей сетей передачи данных благодаря своим преимуществам по сравнению с проводными: простота, дешевизна и быстрота развертывания. Однако, с точки зрения безопасности, технологии, в которых для передачи используется кабель и злоумышленнику для перехвата информации требуется как минимум получить физический доступ к нему, выигрывают у беспроводных технологий. Как правило в технологиях проводных сетей проблемами безопасности передаваемых данных занимаются сервисы и службы верхних уровней, для технологий же, использующих эфирную среду передачи, из-за их доступности и повышенной уязвимости, уже на нижних уровнях (на уровне MAC) используются элементарные механизмы защиты.

На сегодняшний день для организации взаимодействия устройств в IoT используется широкий спектр технологий: BluetoothLE (LowEnergy), ANT, ZigBee, RF4CE (RadioFrequencyforConsumerElectronics), Wi-Fi (IEEE 802.11v), Nike+, IrDA (InfraredDataAssociation), NFC (NearFieldCommunication). В докладе дается обзор популярных в интернете вещей технологий беспроводного доступа и рассматриваются предлагаемые ими средства защиты от несанкционированного доступа.

Верзун Н.А., Колбанев А.М., Колбанев М.О
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
Объединенная компания Дом.ru InterZet

АСПЕКТЫ БЕЗОПАСНОСТИ В ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ» ОБРАЗОВАТЕЛЬНОГО НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

В соответствии с Федеральным государственным образовательным стандартом III-го поколения по направлению подготовки бакалавров «Информационные системы и технологии» одной из базовых дисциплин общепрофессиональной части учебного плана является дисциплина «Инфокоммуникационные системы и сети», читаемая студентам в 7 семестре.

Материал учебных пособий по данной дисциплине должен развивать фундаментальные знания информатики в области инфокоммуникаций и обобщать опыт прикладных разработок в данной области, а также давать представление о современном состоянии теоретических и прикладных вопросов, связанных с процессами и технологиями распространения информации, об идеологии построения инфокоммуникационных систем и сетей, математическом аппарате моделирования сетей методами теории телетрафика, о возможностях и путях использования инфокоммуникационных технологий при построении современных распределенных систем. Одной из главных проблем, которую необходимо решать при создании, внедрении и сопровождении инфокоммуникационных систем и сетей, является задача обеспечения их защиты и информационной безопасности. Именно поэтому, целесообразно при изучении дисциплины “Инфокоммуникационные системы и сети” аспектам безопасности выделить отдельный раздел.

План изложения материала по дисциплине «Инфокоммуникационные системы и сети» может быть, например, следующим:

1. История и перспективы развития систем и сетей распространения информации. В рамках данного раздела можно провести небольшой исторический экскурс в этапы развития и становления инфокоммуникационных систем и сетей, изложить задачи и особенности современных телекоммуникационных сетей, дать основные понятия и определения, связанные с такими терминами как информация, информационное взаимодействие, телекоммуникационные услуги, качество услуг и др., а также коснуться вопросов государственного управление в области связи.

2. Инфокоммуникационные процессы. Необходимо остановится на проблемах конвергенции и интеграции информационных процессов и технологий, рассказать об особенностях предоставления инфокоммуникационных услуг, а также изложить концепцию открытых систем.

3. Инфокоммуникационные технологии. Рассматриваются следующие технологии: технологии переноса информации, мультиплексирования линий связи, коммутации и множественного доступа.

4. Инфокоммуникационные сети. Предлагается рассмотреть следующие типы сетей: первичные сети (например: сети PDH/SDH и ATM), телефонные проводные сети и сети связи мобильных абонентов, локальные сети и сети доступа, телевизионные и радиовещательные сети. Также необходимо уделить внимание вопросам объединения сетей на основе базовых протоколов интернет.

5. Инфокоммуникационные системы. В данном разделе рассматриваются: системы нумерации и адресации, управления и технического обслуживания, системы учета стоимости и расчетов с абонентами и др.

6.Безопасность и защита в инфокоммуникационных системах. Необходимо изучить следующие вопросы: виды и источники угроз безопасности информации. Методы защиты информации: программные и аппаратные средства. Защита информации в локальных и глобальных сетях: разграничение доступа между сетями. Использование межсетевых экранов. Возможности фильтрации трафика на канальном, сетевом, транспортном и прикладном уровне.

7. Элементы теории телетрафика. Здесь излагаются теоретические основы моделирования инфокоммуникационных сетей как систем массового обслуживания. Даются основные понятия теории телетрафика (поток заявок на обслуживание, свойства и типы потоков, время и дисциплина обслуживания и пр.).

Верзун Н.А., Колбанев А.М., Колбанев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
Объединенная компания Дом.ru InterZet

ЭНЕРГЕТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

В последние годы наблюдается значительное увеличение затрат на реализацию процессов информационного взаимодействия посредством информационных технологий. В связи с этим актуальной для специалистов информационной сферы становится задача обеспечения экономии физических ресурсов обеспечивающих подобное взаимодействие. Физические ресурсы, к которым относят пространственные, временные и энергетические, затрачиваются на всех этапах информационного взаимодействия, а именно, на этапах распространения, сохранения и обработки информации.

Современные информационные системы (как глобальные, так и локальные), в основном, базируются на использовании технологии коммутации пакетов, и разрабатывались и создавались они в прошлом веке. Тогда еще никто не задумывался о пределах закона Г. Мура, в соответствии с которым объемные характеристики информационных систем росли экспоненциально (в 2007 г. Г.Мур предположил, что предложенный им закон вскоре перестанет действовать т.к. существует предел возможностей современных полупроводниковых технологий). Задачи, стоявшие в то время перед разработчиками, были: обеспечение совместной работы неоднородных сетей, повышение коэффициента использование оборудования, экономия пропускной способности каналов, обеспечение информационного взаимодействия в реальном времени и пр. Однако, в настоящее время все большее значение приобретает задача повышения энергоэффективности информационных сетей.

К числу главных причин энергетической неэффективности мощных информационных систем относятся затраты на распространение данных и сложность аппаратно-программного обеспечения интерконнекта, решающего эти задачи. Одним из путей повышения энергоэффективности технологий распространения является рациональный выбор алгоритмов управления информационными потоками. А именно алгоритмов: выбора эффективной длины передаваемых блоков, доступа к среде передачи, передачи сообщений по сети, передачи и обработки служебной информации, сжатия, шифрования информации и пр.

Рассматриваются сетевые технологии, в частности, информационные системы множественного доступа, с точки зрения энергии, потребляемой центрами коммутации и обработки информации в процессе оказания телематических услуг пользователям. Учитываются два основных процесса пакетной коммутации: обработка адресов и другой служебной информации в процессе информационного взаимодействия, и формирование линейного кода для транспортировки данных.

Для математического моделирования процессов старения информации используется аппарат систем массового обслуживания в дискретном времени. Предполагается: однородная локальной сети передачи данных, метод доступа – синхронный временной, используется режим пакетной передачи, при котором файл для передачи разбивается на равные части(блоки). Предлагаются выражения для расчета характеристик передачи файла по сети: вероятностно-временных и энергетических.

Исследуется влияние длины передаваемого блока информации в локальной сети передачи данных, а также качества среды передачи на вероятностно-временные(вероятность своевременной доставки файла) и энергетические характеристики (энергозатраты на обработку служебной информации и формирование линейного кода) передачи файла по локальной сети.

Воробьев А.И. Колбанёв А.М.,Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Объединенная компания Дом.ru InterZet, Санкт-Петербургский государственный экономический университет

ОПТИМИЗАЦИЯ ИНФРАСТРУКТУРЫ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

В докладе обсуждается вопрос оптимизации инфраструктуры центра обработки данных (ЦОД).

Сформулирована задача оптимизации эффективного и сбалансированного ЦОД в терминах смешанного программирования, одновременно дискретного, целочисленного и непрерывного типа. Такие переменные, как изменяемое в процессе оптимизации число серверов, кластеров, систем хранения, коммутаторов и каналов связи относится к классу целочисленных, а выбор пропускных способностей и производительности элементов ЦОД осуществляется из некоторого дискретного ряда.

Анализируются различные архитектуры серверов, систем хранения данных и коммутаторов, способствующих балансировке нагрузки на узлы ЦОД.

К непрерывным переменным относятся различные вероятностно-временные характеристики. Оценка характеристик выполняется с применением моделей систем и сетей массового обслуживания.

В условиях отказоустойчивого функционирования ЦОД предлагается генетический алгоритм, который распределяет задачи с отказавших серверов на работоспособные.

Показано, что рациональной является инфраструктура ЦОД, которая не только позволяет выполнять текущие задачи, но и обеспечивает дальнейшее развитие, с учетом роста объемов информационных услуг и повышения требований к показателям качества по предоставлению услуг.

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

ОПТИМИЗАЦИЯ ПРОЦЕССА СЖАТИЯ ДАННЫХ ПО КРИТЕРИЮ ЭНЕРГОПОТРЕБЛЕНИЯ

Доклад посвящен проблеме оптимизации энергопотребления в интернете вещей.

Объектом исследованияявляются умные вещи, представляющие собой терминальные устройства интернета вещей, создание которого относится к числу самых актуальных направлений развития информационных технологий. Предметом исследования являются энергетические ресурсы, необходимые для работы умных вещей. Цель заключается в построении модели информационных процессов, позволяющей оптимизировать энергопотребление умными вещами.

Умная вещь – это относительно новый тип сетевых устройств. В соответствие с рекомендацией МСЭ, главные их признаки – это наличие уникального идентификатора и возможность подключения к сети связи. Количество вещей, подключенных к сетям, превысило количество людей в 2009 г., а к 2020 г. превысит уже на несколько порядков. По прогнозам интернет вещей станет крупнейшей составной частью рынка ИТ в ближайшие 10 лет, реализация этой концепции принесет $14 триллионов выручки. Примером умных вещей служат интернет счетчики, датчики-переключатели, брелки локальной навигации, медицинские приборы на теле человека, приборы для мониторинга окружающей среды, контроля над животными или автомобилями, умная пыль и так далее.

Предложена модель для оценки и оптимизации энергопотребления умными вещами на этапах сжатия и передачи данных, приводится численный пример выбора варианта организации информационных процессов для умных вещей по критерию энергопотребления.

ВоробьёвА.И., Колбанёв А.М., КолбанёвМ.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Объединенная компания Дом.ru InterZet, Санкт-Петербургский государственный экономический университет

АНАЛИЗ ХАРАКТЕРИСТИК ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ С НЕОРДИНАРНЫМ ПОТОКОМ ЗАЯВОК НА ОБСЛУЖИВАНИЕ

В докладе представлены результаты анализа вероятностно-временных характеристик инфокоммуникационной системы, использующей при обслуживании заявок алгоритмы коммутации с установлением соединения. Показано, что процесс обслуживания неоднородного потока заявок, требующих разной скорости передачи при предоставлении услуг разного типа, может быть описан при помощи СМО с неординарным потоком заявок на обслуживание.

Дается описание программных средств расчета и имитационного моделирования. Приводятся полученные с их помощью оценки вероятностей блокировки разнородных заявок от интенсивности суммарного потока, неординарности заявок, соотношения интенсивностей поступающих потоков, скорости канала связи, среднего времени предоставления услуг разного типа, алгоритма повторных попыток занятия ресурсов, доступности сетевых ресурсов и др.

Проведенный анализ позволяет сделать вывод о необходимости учета взаимной зависимости характеристик качества обслуживания заявок разного типа друг на друга на этапах разработки, проектирования и эксплуатации инфокоммуникационных систем.

Воронина Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ УГРОЗ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Информационно-экономическая безопасность корпораций в определенной степени определяется отказоустойчивостью и надежностью информационных систем.

Глобализация бизнеса, широкое использование интернета, мобильные вычисления, ориентация на заказчика — все эти тенденции требуют отказоустойчивого, бесперебойного функционирования компьютерных систем. Решения зависят от вычислительных систем — их надежности и способности к безостановочной работе 24 часа в сутки. Рост сложности и объемов

вычислений тормозят этот процесс. Издержки из-за неисправности техники растут, а вместе с ними и потери, связанные с финансами и ущербом репутации исполнителей. Ведь даже несколько минут простоя важных систем могут иметь катастрофические последствия, которые выражаются в упущенных деловых возможностях, снижении уровня доверия заказчиков и в прямом ущербе деловой репутации компании.

Работоспособность информационной системы предприятия является определяющим фактором эффективности его деятельности, что диктует необходимость построения таких систем, которые основаны на современных технологиях и обеспечивают характеристики известные, как «RAS» (Reliability, Availability, Serviceability — Надежность, Готовность, Удобство обслуживания). Эти характеристики являются традиционными для современных систем.

Выбор надежного оборудования и ПО позволяет до определенной степенипредотвратить сбой информационной системы. Однако встречаются и неподвластныесистемному администратору ситуации, влекущие за собой уничтожение информационнойсистемы или какой-либо ее части. В условиях сложных деловых связей «падение» однойкомпании, ставит под удар функционирование многих ее партнеров. Поэтому задачаруководства компании — заранее определить ряд мероприятий, составляющих план восстановления бизнеса после катастрофы (или BusinessDisasterRecovery, BDR), которыепозволяют свести к минимуму потери информации и время простоя системы.

Вместе с ростом роли информационных систем в обеспечении качества продукции и услуг предприятия и организации происходит рост рисков, связанных с недоступностью данных и информационных служб, необходимых для осуществления поддержки процессов жизненного цикла. Непрерывность и качество этих процессов находится в прямой зависимости от доступности информационной системы предприятия. Допустимое время простоя информационных служб и недоступности данных определяется исходя из характера задач, решаемых информационной системой.

Головкин Ю.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

СИТУАЦИОННЫЕ МОДЕЛИ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СИСТЕМАМИ

Надежность и безопасность эксплуатации сложных технических системво многом зависит от правильного и своевременного выбора управляющих действий для достижения цели функционирования. Разработка моделей и программных средств, повышающих качество формирования управляющих воздействий для обеспечения эффективного автоматизированного управления техническими системами, является важной и актуальной задачей.

Современные технические системы характеризуются многоуровневой структурой, большим количеством взаимодействующих и взаимосвязанных элементов, разнообразием режимов функционирования. Особенностью многих технических систем является дискретный характер управления. Процесс управления системами подобного класса можно представить в виде последовательной смены ситуаций, требующих вполне конкретных управляющих действий. При организации автоматизированного управления такими системами целесообразно и эффективно использовать ситуационный подход. Под ситуацией понимается состояние процесса управления, характеризующееся определенными параметрами функционирования объекта управления и определяющее необходимые управляющие действия (команды управления, сообщения оператору).

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 .Предикат – это логическая функция, заданная на множестве значений параметров функционирования объекта управления, которая определяет активность соответствующей дуги модели. Кроме того, дуги помечаются символами, которые определяют управляющие действия. Также дугам могут быть присвоены приоритеты. При этом значения приоритетов для всех дуг, исходящих из одной вершины, должны быть различны.

Одна из вершин модели выбирается в качестве первой и соответствует начальной ситуации. Выявлено, что для адекватного описания процесса управления ситуационная модель может иметь многоуровневую структуру, при которой любой вершине (ситуации) ставится в соответствие некоторая внутренняя модель.

Разработан алгоритм обработки ситуационной модели. Обработка начинается с начальной вершины ориентированного графа. Далее производится проверка значений предикатов исходящих дуг. Если предикат истинен, то производится переход к обработке следующей вершины. Если же предикат ложен, то происходит проверка на активность других исходящих дуг данной вершины графа .Аналогичным образом производится обработка всех уровней модели. Таким образом, на каждом такте работы формируются выходные управляющие действия и корректируется текущая ситуация процесса управления.

Рассматриваются вопросы программной реализации разработанного алгоритма и моделирования процесса управления 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 конечном итоге можно отметить, что использование ситуационных моделей приводит к повышению качества формирования управляющих действий и увеличивает эффективность автоматизированного управления техническими системами в целом.

Гусева Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И РИСКИ ПРИ СОВЕРШЕНИИ СТАВОК НА СПОРТИВНЫХ МАТЧАХ

В современном информационном обществе мы все больше обращаем внимание на дополнительный заработок в Интернете. А при развивающемся интересе к спорту в нашей стране многие видят решение своих финансовых проблем именно в ставках на результаты спортивных матчей. На данный момент этот рыночный сегмент наполняют букмекерские конторы, многие из которых не дают гарантию своим игрокам. А каждый из игроков хочет быть уверен, что не потеряет свои деньги из-за собственной беззаботности или ошибки букмекеров. Интерес и тяга к прибыли в этой игре есть у обеих сторон линии букмекер-клиент, поэтому должно присутствовать взаимное доверие при размещении спортивных ставок. Игроки, со своей стороны хотят получать своевременные выплаты своего выигрыша на указанный счет, а конторы стараются удовлетворить клиентов и повысить имидж компании для привлечения новых игроков. В связи с этим последние расширяют свои партнерские отношения с различными системами оплаты, причем, не все из них являются надежными. Чтобы проверить надежность букмекерской конторы, с которой работает клиент, нужно просмотреть множество сайтов, форумов, где можно найти необходимую информацию и мнения как простых игроков, так и экспертов в данном вопросе. Существует также и специальный рейтинг SBR, который дает полное понимание того, с какой конторой мы имеем дело.

Как и множество различных азартных игр, ставки на спорт имеют огромное количество проблем в рамках безопасности: букмекеры часто обманывают своих игроков, создавая свои правила и дезинформируя клиентов; имеют дело с непроверенными серверами оплаты, выплаты, денежных средств; занижают или наоборот повышают коэффициенты экспертов и их прогнозы на матчи. Также предоставляют ненадежный сервис ставок в интернете.

По данным маркетинговых исследований, ставки на спорт имеют большую развлекательную ценность в связи с проникновением в Интернет. Большинство букмекерских контор уже перешли от терминалов к онлайн сервисам, возрастающая конкуренция дает нам сигнал больше обращать внимания на управление своими рисками при работе с букмекерами. В данной работе мы исследуем преимущества использования статистически приемлемых моделей при совершении ставок в качестве поддержки принятого решения и исследуем факторы, которые привели нас к такому выводу, а также потенциал данных моделей, чтобы повысить их точность.

Задачей данной работы является разработка универсального механизма совершения ставок на сайте букмекерской конторы без обмана и потери денежных средств. Проведение анализа деятельности различных «поставщиков», действующих на данном рынке выполняется сравнением их с помощью критериев отбора букмекерских контор. Рассмотрение наиболее надежные и популярные систем оплаты ставок. При регистрации нового игрока букмекеры устанавливают проверку счета пользователя. Чтобы быть обезопасить свой счет на сайте букмекерской конторы необходимо знать про эту контору все и следить за ее деятельностью постоянно, так как все может измениться, а мы хотим знать, что наши финансы в безопасности. В проверке есть свои плюсы: мы будем уверены, что в случае взлома нашего счета и попытке вывода средств сложно будет обмануть онлайн букмекера, который обязательно потребует выслать копии паспорта и кредитной карты. Но есть и минусы: проверка может продлиться несколько дней; и как понять, что букмекер не обманывает нас и ничего не сделает с предоставленной ему информацией. Для уверенности в этом, пересылая документы, нужно закрывать часть важных данных, о которых букмекер знать не должен. Также обращаем внимание, что ни один работник компании не имеет права спрашивать нас о пароле доступа к счету, а если вдруг такой инцидент произойдет, необходимо доложить службе поддержки клиентов.

Целью использования модели является выработка прибыльной стратегии ставок на футбол с уменьшением риска и выбором безопасного букмекера. Для достижения данной цели мы воспользовались моделью Пуассона (Poisson model) и проследили ее полезность в букмекерском рынке. Также сравнили Пуассоновскую модель с другими, наиболее часто используемыми методами прогнозирования, такие как рейтинги и мульти-модели. В работе охарактеризовано большинство типов ставок с фиксированным коэффициентом, способы его проверки, безопасность букмекера и системы оплаты. Эффективность использования модели в более экзотических видах ставок также кратко обсуждены.

Таким образом, универсальный механизм, или же предложенная модель докажет, что футбольные ставки достаточно прибыльны и безопасны, что она довольно эффективно захватывает многие аспекты и игры и наконец-то позволяет завершать игровые сезоны с положительной прибылью.

Егорова И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОБ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В последние годы в связи с развитием сетевых технологий и распространением мобильных устройств для доступа к данным и их обработки (планшеты, телефоны) изменились требования и подходы, применяемые при разработке корпоративных информационных систем (КИС). Изменения коснулись в основном организации взаимодействия между пользователями и системой (интерфейса) и вопросов связанных с обеспечением информационной безопасности КИС.

Доклад посвящен анализу угроз и методам повышения информационной безопасности КИС.Современные системы управления масштаба предприятия используют распределенные хранилища данных. При этом рассматриваются два основных аспекта обеспечения информационной безопасности: предотвращение несанкционированного доступак информации и обеспечение возможности бесперебойного доступа к данным системы независимо от местоположения пользователя и применяемых им аппаратных средств.

При разработке КИС должны быть определены возможные сценарии работы пользователей с хранилищем информации в зависимости от того работают ли они во внутренней сети предприятия или получают доступ к информации через публичную сеть передачи данных. На этой основе необходимо определить роли пользователей и использовать эту информацию при проектировании архитектуры хранилища данных. Только часть хранилища обычно может быть сделана доступной из публичных сетей. Для защиты внутренней сети предприятия от доступа из внешних сетей используются комплексы программно-аппаратных средств, которые называются межсетевыми экранами.

Часть информации может храниться в зашифрованном виде и расшифровываться только при необходимости доступа к ней, но это требует дополнительных ресурсов, замедляет работу системы и осложняет поиск данных. Поэтому шифрование должно применяться только там, где это действительно необходимо.

Другим важнейшим аспектом информационной безопасности является защищенность ресурсов системы, которые доступны с мобильных устройств через публичные сети. Эти ресурсы являются менее защищенными и могут подвергаться различным видам атак хакеров. Например, результатом DDoS атаки является невозможность получить доступ к ресурсу или для легальных пользователей – «отказ в обслуживании».Также ресурсы, размещенные во внешней сети, подвергаются вирусным атакам с использованием уязвимостей в применяемом программном обеспечении.

Одним из технологических достижений последних лет является широкое применение виртуализации и облачных технологий в КИС. Эти технологии предполагают создание центров обработки данных (ЦОД). Применение ЦОД позволяет оптимально распределять нагрузку на вычислительные ресурсы предприятия, обеспечивает централизованное управление этими ресурсами и в результате позволяет экономить средства, требуемые на приобретение и эксплуатацию КИС. Но использование облачных технологий только повышает важность этих аспектов информационной безопасности.

Обеспечение информационной безопасности в системах управления уровня предприятия возможно только на основе применения комплексного подхода опирающегося на знание стандартов в этой области и использовании современного аппаратного и программного обеспечения.

Емелин В.И., Колмыков Г.Н.
Россия, Санкт-Петербург, ОАО «НИИ Вектор»
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОЭЛЕКТРОННОГО МОНИТОРИНГА

В последние десятилетия Россия была вовлечена в целый ряд гибридных войн, которые на определенных этапах ее ведения отличались различным уровнем использования военных и невоенных инструментов при скрытном и постоянно жестком информационном противоборстве. Роль информационной составляющей является определяющей для успешной реализации концепции «управляемого хаоса», когда дезинформация, также, как и информация, в значительных объемах, неконтролируемо и практически мгновенно может быть поставлена любым потребителям и, что особенно важно, лицам, принимающим решения (ЛПР) в сложной быстроменяющейся обстановке. В этом направлении идет постоянное развитие различных информационных технологий, включая технологии радиоэлектронного противоборства, благодаря чему каждая новая конфликтная ситуация чревата появлением новых нетрадиционных угроз, новых сюрпризов. Решать такие проблемы необходимо до их возникновения на практике. В сфере обороны выполнение финансируемых государством научно-технических и технологических программ требует особого внимания, так как отрасли, производящие знания и информационные продукты, относятся к секторам экономики, снабжающим производство его наиболее существенным ресурсом.При разработке методов и средств защиты от деструктивных информационных воздействий будем исходить из предпосылки, что целью атакующей стороны является дезоптимизация процесса управления у защищающейся стороны: нахождение такой комбинации влияющих независимых переменных, при искажении которых выбранный показатель оптимальности принимает планируемое в результате атаки экстремальное значение ущерба.Решающую роль в этом процессе играет система знаний о радиоэлектронной обстановке (РЭО), которые формируются в процессе сопоставления данных наблюдения и измерения с выдвинутыми гипотезами и являются наиболее устойчивой разновидностью информации.В условиях нарастающего развития средств точечного деструктивного воздействия на процесс принятия решений при мониторинге РЭО рассматривается вариант представления совокупности измеряемых демаскирующих признаков как элементов модели, где действуют следующие его закономерности:

1) Измерению, передаче и обработке подлежит совокупность разнородных данных, свойства которых (полнота, достоверность и оперативность) определяются различными требованиями и условиями эволюции, внутреннего и внешнего воздействия. В результате действия этих факторов значения их свойств являются случайными величинами, которые, тем не менее, изменяются в заданном интервале и известном законе распределения.

2) Требования к качеству добываемой разнородной информации в общем случае также могут быть различными, но вполне конкретными, что при условии наличия или отсутствия разнородных априорных знаний по каждому элементу обстановки определяет детерминированность процесса в широком диапазоне (от полного знания до полного незнания обстановки).

Такое описание протекающего процесса соответствует определению детерминированного хаоса: случайное, непредсказуемое поведение системы, формируется детерминистическими законами в условиях предсказуемой эволюции, управленческих действий и деструктивных внешних воздействий. По результатам проведенных исследований следует выделить следующие особенности современного производства новых наукоемких информационных технологий в области радиоэлектронного мониторинга:

– теоретические знания являются основой технологических инноваций, их накопление на производстве связано с увеличением затрат в человека в интересах создания «интеллектуального капитала»;

– в структуре производства формируются устойчивые доминирующие группы, состоящие из работников нового типа - разработчиков знаний («knowledgeworker»);

– растущая сложность, ограниченность ресурсов и системность инноваций требуют создания производства на основе новой технологической парадигмы массового применения распределенных ресурсов глобальных сетей;

– создание информационных технологий зависит, прежде всего, от наукоемких активов (знаний, опыта, ноу-хау и т.д.), которые стимулируют развитие инноваций и рост потребительской стоимости товаров и услуг.

Емельянов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Доклад посвящен анализу существующего положения в сфере защиты передаваемых данных при использовании беспроводных сетей стандарта IEEE 802.11.

Показано, что передача информации при неуклонно растущем сегменте локальных и глобальных сетей с технологией Wi-Fiтребует усиленных мер для обеспечения конфиденциальности.

Достижения в сфере беспроводной передачи данных вкупе с удешевлением персональных устройств, использующих протоколы 802.11, существенно расширили область применения указанной технологии. Если в 2000-ых годах сети Wi-Fiпредставляли собой лишь малую часть всего многообразия компьютерных сетей, то на текущий момент устройства с модулями беспроводной передачи данных занимают более 50% рынка (особенно ус-ва мобильного типа: коммуникаторы, планшеты, нетбуки, смарт-гаджеты и т.д.)

В отличие от классических проводных решений, для подключения к сетям стандарта 802.11 отсутствует необходимость использования специального кабеля, соединяющего конечные устройства пользователей с беспроводной точкой доступа. Данный факт означает, что коммерчески значимая информация (как и любая другая - например, компрометирующая человека или группу лиц) может быть перехвачена злоумышленником, не находящимся непосредственно на территории расположения того или иного предприятия, достаточно лишь оказаться в радиусе действия специализированного устройства (точки доступа либо маршрутизатора, имеющего модуль Wi-Fi), выполняющей роль сетевого коммутатора.

С целью недопущения утечки конфиденциальных данных необходимо применять различные системы защиты передаваемой информации. Специфика же заключается в том, что при отсутствии прямого физического подключения возрастает сложность контроля устройств, связанных между собой. Данная проблема требует детальной проработки политик сетевой безопасности, направленных, с одной стороны, на беспрепятственный доступ уполномоченных сотрудников к внутри- и внешнесетевым ресурсам, с другой – на запрет как случайных подключений, так и преднамеренных, имеющих целю перехват данных.

Для достижения данной цели необходимо реализовать:

- контроль доступа, базирующийся на аутентификации пользователей;
- потоковое шифрование трафика с использованием криптографически надежных протоколов;
- систему предотвращения вторжений в беспроводную сеть;
- систему обнаружения чужих устройств и возможности их активного подавления;
- мониторинг уязвимостей в беспроводной сети и возможности аудита уязвимостей.

Аутентификация позволяет проверить, имеет ли право устройство либо пользователь подключаться к внутренним ресурсам. Потоковое шифрование трафика предназначено для блокировки возможности перехвата и использования данных, транслируемых через радиоканал. Система предотвращения вторжений контролирует внутрисетевые потоки данных и отсекает подозрительную активность. Система обнаружения чужих устройств сканирует в реальном времени радиочастотные диапазоны в рамках стандарта 802.11 и локализует устройства, не относящиеся к зарегистрированным, после чего блокирует возможность их подключения к внутрисетевым ресурсам. Мониторинг уязвимостей предназначен для определения потенциальных опасностей внутри сети и оперативного устранения либо сведения их к минимуму.

Емельянов А.А., Коршунов И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОПЫТ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ МАЛОГО БИЗНЕСА В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Переход от индустриального к информационному обществу ознаменовался возрастанием роли информации во всех сферах человеческой деятельности, в частности в экономике. Информатизация общества стала причиной глобализации экономики. Глобализация экономики, в свою очередь, выдвинула на первый план вопросы экономической безопасности. Предприятие является субъектом экономической системы, поэтому вопросы обеспечения его экономической безопасности являются актуальными.

Информационно-экономическая безопасность неразрывно связана с понятием угрозы как совокупности условий, факторов и событий, которая определяет эффективность внутренних и внешних деструктивных информационных воздействий на экономическое состояние предприятия. Иными словами, угроза информационно-экономической безопасности – это реальные или возможные действия (события) в отношении информации, которые могут привести к нарушению целостности, устойчивости или саморегуляции экономической деятельности предприятия. Противодействие информационным угрозам в сфере экономики является одной из задач информационно-экономической безопасности. Вариантом ее решения может быть разработка и внедрение политики безопасности на предприятии.

Политика информационной безопасности является организационным документом, который регламентирует деятельность отдельных подразделенийи организации в целом в рамках использования информационной системы предприятия.

Существующие подходы обеспечения информационно-экономической безопасности были учтены при разработке политики информационной безопасности малого предприятия «СпецСервис». ООО «СпецСервис» с головным офисом в Санкт-Петербурге выполняет посреднические услуги на рынке металлопроката. В состав информационной системы предприятия входит аппаратно-программный комплекс, состоящий из ряда рабочих станций, выделенных серверов и гетерогенной локальной вычислительной сети, связывающей как устройства внутри офисов предприятия, так и реализующей подключения региональных отделений компании и сотрудников, работающих по удалённой схеме. Проведенное обследование предприятия позволило выявить слабые места с точки зрения информационной безопасности:

– коммерчески значимой информацией, подлежащей защите, является база поставщиков и клиентов, динамически изменяющаяся в зависимости от временных факторов, состояния рынка металлопроката, ценообразования и иных параметров;

– текущая конфигурация АПК и ЛВС практически не защищена как от хищения информации, так и от псевдослучайных повреждений данных.

В качестве угроз безопасности информации были определены:

– несанкционированный доступ/копирование/изменение коммерчески важной информации;

– повреждение данных из-за сбоев аппаратно-программной базы.

По результатам обследования руководством предприятия было принято решение о разработке и внедрении системы безопасности, реализующей защиту, как персональных данных пользователей, так и базы данных компании. Создание системы безопасности на предприятии началась с разработки политики информационной безопасности, целью которой являлось сведение к минимуму потенциальных уязвимостей, выявленных в результате обследования. Для этого необходимо было решить следующие задачи:

– построение схемы локальной сети предприятия, учитывающей рабочие станции, серверы, систему удалённого подключения;

– локализацию уязвимостей на уровне конечных устройств и на уровне ЛВС;

– выбор необходимых аппаратных и программных решений, позволяющих минимизировать уязвимости;

– конфигурирование аппаратно-программной среды для внедрения вышеуказанных решений.

Разработанная политика информационной безопасности была внедрена на предприятии. За прошедший с момента внедрения год система безопасности работает удовлетворительно, сбои отсутствуют, хищений информации не отмечено. Все потенциально опасные действия пользователей, выходящие за рамки должностных инструкций, определяются и пресекаются на этапе формирования.

Желваков Б.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

КОРПОРАТИВНЫЕ ЗНАНИЯ В АРХИТЕКТУРЕ СОВРЕМЕННОГО ПРЕДПРИЯТИЯ

С переходом к экономике, основанной на профессиональных знаниях и информационных технологиях одной из самых актуальных стратегических целей современного предприятия становится выявление, накопление и управление активами корпоративных знаний. Благодаря высокому уровню корпоративных знаний, предприятия становятся более эффективными, особенно в использовании дефицитных ресурсов, и наоборот, без таких знаний предприятия утрачивают свою эффективность, терпят неудачу в условиях быстро-меняющихся и высоко конкурентных рынков.

В докладе представлена полнокомпонентная архитектурная (комплексная) модель современной автоматизированной производственной системы, приведены определения понятий «корпоративная информация», «корпоративныеые знания», «корпоративная база знаний» и кратко охарактеризован архитектурный компонент «Архитектура знаний».

Под корпоративной информацией следует понимать такие данные, сведения которые несут правдивое, своевременное описание производственной системы и различных ситуаций её деятельности, причём эти сведения организованы так, что они имеют определённую «смысловую» ценность (в смысле новизны и полезности) для всех работников предприятия и прочих заинтересованных лиц (Stakeholders) – собственников (акционеров), руководителей всех уровней и разработчиков управленческих информационных систем.

Корпоративные знания отражают не только «смысловое» содержание особым образом организованных данных и сведений, но и накопленный жизненный опыт и результаты профессионального обучения *всех* работников предприятия (основных, управленцев всех уровней и даже вспомогательных). Определение корпоративных знаний можно сформулировать следующим образом:Корпоративные знания – это информация, декларативная часть которой организована в традиционных и специализированных базах и хранилищах структурированных и неструктурированных данных и базах знаний, а процедурная – в программных компонентах автоматизированной управленческой системы, а также в сознании всех сотрудников предприятия, проанализирована

экспертами предметных областей, в которых функционирует такое предприятие, с целью сделать ее понятной и применимой для решения аналитических, прогностических и других управленческих задач или принятия управленческих и иных решений.

Основу корпоративных знаний обеспечивает среднее и высшее профессиональное обучение. Конкретизация, уточнение и регулярное совершенствование этих знаний должно выполняться в процессе организационного обучения на конкретном предприятии.

Предприятия совершенствуют корпоративные знания с помощью разнообразных организационных механизмов обучения. Способность организации обучаться на основе информации о своей среде, а также включать знания в выполняемые бизнес-процессы повышает эффективность управления знаниями. С помощью метода проб и ошибок, тщательной оценки запланированных действий и обратной связи производителя с потребителями (и, в целом, – с окружающей средой организации) разрабатываются новые стандартные операционные процедуры и бизнес-процессы, отражающие опыт их применения. Этот процесс называется «организационным обучением». Очевидно, что организации, способные быстро обнаруживать и реагировать на изменения внешней среды, выживут во всё обостряющейся конкурентной борьбе дольше организаций со слабыми механизмами обучения.

Учёт активов корпоративных знаний привёл к появлению в информационной архитектуре предприятия компонента «Архитектура знаний», а в программной структуре КИС – систем обработки знаний, коллективного сотрудничества и компонента «Управление знаниями» (Knowledge Management – KM).

Иванов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ОЦЕНКА СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ АСПЕКТОВ БЕЗОПАСНОСТИ СТРАН ЕАЭС

Европейско-азиатское экономическое сообщество (ЕАЭС) возникло, прежде всего, как фактор содействия экономическому развитию стран евроазиатского континента. После преодоления естественных проблем «болезней роста» его вклад в развитие мировой экономики будет неуклонно увеличиваться.

Социально-экономические факторы, в том числе такие, как средний уровень зарплат, пенсий, валовый национальный продукт на душу населений, внешний государственный долг на душу населения (см.[http://ru.sputnik.kg/infographics/ 20150508/1015437308.html, 24 июня 2015 г.]), оказывают влияние не только на развитие стран, но и на общее состояние безопасности государств.

Рассмотрим влияние валового внутреннего продукта на душу населения и внешнего государственного долга на душу населения на среднюю зарплату жителей стран ЕАЭС. Проведем регрессионный анализ, представив среднюю зарплату в виде линейной свертки: $y = C1\ x1 + C2\ x2 + C3$, где y – средняя зарплата, x1 – валовой внутренний продукт на душу населения, x2 – внешний государственный долг на душу населения, C1, C2, C3 – весовые коэффициенты, которые находятся из решения соответствующей системы линейных уравнений. Коэффициент C3 описывает влияние неучтенных факторов. После расчетов получим следующие значения коэффициентов: C1 = 46,084, C2 = -51,169, C3 = 212,731. Домножим эти коэффициенты на значения математических ожиданий параметров и сложим. Получим результирующее значение. Если на него поделить каждое произведение, то у нас будет относительный вклад в результат, соответственно равный: 0,648, – 0,126, 0,478. Они говорят о том, что наибольшее влияние (64,8%) оказывает валовой внутренний продукт на душу населения, обслуживание внешнего долга составляет только 12,6%. Влияние неучтенных факторов – 47,8%. Для их детализации требуется дополнительная информация. Если рассмотреть влияние тех же параметров на пенсию, то относительный вклад в результат будет следующим: 0,678, – 0,0383, 0,360. Считая, что погрешность исходной информации не превосходит 5%, можно сделать вывод о том, что на уровень пенсии обслуживание внешнего долга стран ЕАЭС практически не оказывает никакого влияния. Отсюда можно сделать следующий вывод о том, что обслуживание внешнего долга само по себе в меньшей степени оказывает влияние на социальное напряжение населения стран ЕАЭС.

Домножим значения коэффициентов разложения средних зарплат на соответствующие значения параметров. Получим расчетные значения средних зарплат. Сопоставим их с фактическими.

Анализ результатов вычислений показывает, что у Армении средняя зарплата превышает расчетную на 18,5%, т.е. экономическое развитие страны приносится в жертву социальному обеспечению населения. Россия имеет некоторое превышение фактической зарплаты над расчетной (4,4%), что вполне укладывается в оценочную точность информации. У Казахстана расчетная зарплата на 2,6% превышает фактическую. Все это говорит о сбалансированности социально-экономического развития этих стран. У Беларуси и Кыргызстана фактическая зарплата,

соответственно, на 11,4%, и 16,4% ниже. Т.е. в этих странах есть некоторый резерв повышения зарплаты для обеспечения стабильности общества.

Иванов М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ЭНЕРГОЭФФЕКТИВНОСТЬ ТЕХНОЛОГИЙ КОММУТАЦИИ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Доклад посвящен одному из аспектов проблемы обеспечения экологической безопасности информационных технологий – оптимальной организации информационных процессов по критерию потребления электроэнергии. В современном мире стоит проблема в создании таких технических средств, которые не просто обеспечивают эффективную поддержку информационного взаимодействия людей, но и потребляют рациональные объемы физических ресурсов.

В докладе показано, как можно организовать информационные процессы и снизить энергопотребление оборудования при передаче данных в сети.

Колбанёв А.М.
Россия, Санкт-Петербург, Объединенная компания Дом.ru InterZet
ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В докладе информационные технологии рассматриваются с позиции угроз, которые они создают для природной среды и жизненно важных интересов человека.

Показано, что сложившееся в XX веке деление технологических процессов на энергоемкие и информационные (безопасные, неэнергоемкие), уже не соответствует масштабам информационного пространства. Объемы данных, которыми необходимо управлять в процессе человеческой деятельности, достигли астрономических значений и растут экспоненциально. Малая энергия и малые экологические риски в условиях управления малыми информационными потоками, перерастают в большую проблему, вслед за увеличением объема и интенсивности этих потоков и охватываемой ими территории.

Эффективность эксплуатации мощных распределенных инфокоммуникационных систем все больше зависит от энергопотребления и становится существенно выше при использовании выделяемого ими тепла другими технологическими процессами. Даже небольшое снижение удельного потребления электричества в этой сфере заметно снижает выбросы вредных веществ и приводит к колоссальной экономии средств.

Все это заставляет рассматривать информационные технологии не только как инструмент для автоматизации информационного взаимодействия людей в ходе их предметной деятельности, но и как хозяйственную деятельность, способную нанести существенный вред человеку и окружающей среде.

Объектом исследования в настоящем докладе являются базовые информационные технологии (ИТ) сохранения, распространения и обработки данных, а предметом – физические временные, пространственные и энергетические ресурсы, необходимые для реализации этих технологий.

Цель работы заключается в анализе путей создания зеленых информационных технологий и выработке рекомендаций по экономии ресурсов, потребляемых информационными системами. Поставленная цель достигается в результате решения следующих задач:

– общий анализ проблемы создания зеленых ИТ;
– оценка объемов физических ресурсов, требуемых ИТ;
– классификация и анализ путей уменьшения объемов физических ресурсов, потребляемых ИТ.

Приводится пример оценки зависимости энергопотребления инфокоммуникационной сети от параметров процесса распространения данных.

Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ФИЗИЧЕСКИЕ РЕСУРСЫ ИНФОРМАЦИОННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Доклад посвящен анализу объемов физических ресурсов, которые требуются системам хранения данных (СХД).Предлагается разделить эти ресурсы на три типа:пространственные; временные и энергетические.

Пространственные ресурсы определяют объем сохраненных данных и плотность записи, временные – время хранения данных и время доступа к ним, энергетические – прежде всего энергетический барьер, который отделяет минимальные единицы хранения (единица, которая сопоставляется каждому биту информации на цифровых носителях) друг от друга.

Предлагается ввести категории (уровни) данных в зависимости от времени их хранения:

1 уровень – до 1 года. Это так называемые исходные данные, постоянно использующиеся для обработки. Для такой системы такая характеристика, как плотность записи имеет невысокий

приоритет, однако время доступа к информации должно быть минимальным, т.к. работа с такими данными происходит в режиме реального времени. Эти исходные данные как правило хранятся в центрах обработки данных (ЦОД), в качестве носителя в данном случае используются RAID массивы, которые могут обеспечить минимальное время доступа.

2 уровень – от 1 года до 10 лет. К этой категории относятся резервные копии. Время доступа должно быть невелико, чтобы обеспечить быстрое восстановление данных при их потере, однако оно будет существенно больше, чем время доступа для исходных данных. Резервные копии хранятся в системах хранения данных, в качестве носителя в данном случае можно использовать, например, магнитную ленту, магнитооптический накопитель или твердотельный накопитель. Также для хранения больших объемов данных возможно использование биоматериала.

3 уровень – от 10 до 100 лет. К этой категории относятся архивные данные. В данном случае целесообразно использовать CD/DVD/BD библиотеки и библиотеки, основанные на M-дисках, также возможно применение твердотельного накопителя.

4 уровень – более 100 лет. Это данные, для передачи следующим поколениям. Они должны храниться от 100 до 1000 и более лет. При таком длительном хранении сложно обойтись без передовых технологий, таких как стеклянный и вольфрамовый диски, а также записи в ДНК бактерий.

Показано, что существует зависимость между физическими ресурсами. Так, при увеличении времени хранения и увеличении плотности информации снижается время доступа и увеличивается энергия, затрачиваемая на преодоление энергетического барьера. Например, для сохранения данных на 1 миллион лет нужен барьер 60 -70 КВт (более 80 л.с.).

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

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Доклад посвящен анализу проблем безопасности информационного общества.

Показано, что одним из ее критических элементов является пограничная область двух предметных областей: информационной безопасности и экономической безопасности. Водится понятие информационно-экономической безопасностикак комплексной проблемы, заключающейся в защите жизненно важных интересов информационного общества в экономической сфере от внутренних и внешних информационных угроз.

Объектом исследований новой области научных знаний должна стать экономическая система информационного общества. Предметом исследований – состояние ее инфокоммуникационной инфраструктуры, обеспечивающей эффективное циркулирование внутренней информации и защиту от внешней информации влияющих на целостность, устойчивость и саморегуляцию экономической системы. При этом под информационным обеспечением экономической системы предлагается понимать средства, методы и способы отображения достоверной информации о субъектах экономической системы и информационных процессах их взаимодействия, а под экономическим обеспечением информационной инфраструктуры – совокупность ограничений, накладываемых на процессы экономической деятельности, гарантирующих целостное состояние инфокоммуникационной инфраструктуры государства.

Основной цельютеории информационно-экономической безопасности должно стать не просто описание информационных взаимоотношений в экономике, а обоснование их взаимосвязи и взаимообусловленности с состоянием безопасности информационного общества, т. е. раскрытие закономерности информационных воздействий на широкий круг общественных явлений и процессов.

В числе главных задач теории информационно-экономической безопасности можно выделить:

– изучение влияния параметров формирующегося информационного общества на темпы развития экономики страны, регионов, корпораций и отдельных хозяйствующих субъектов;

– выявление механизмов формирования и развития внутренних и внешних информационно-экономических угроз;

– выявление закономерностей информационного воздействия на мировоззрение экономической элиты страны;

– изучение методов информационной борьбы в сфере экономики;

– обоснование методов противодействия информационным угрозам в сфере экономики.

Для проведения научных исследований в этой области необходимы совместные усилия различных специалистов, в первую очередь специалистов информатиков, экономистов, юристов и др.

Колбанёв М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ

Доклад посвящен особенностям процесса информатизации, характерным для современного этапа развития инфокоммуникационных технологий.

Показано, что ближайшие годы станут переломными при переходе к новой третьей платформе информатизации, элементами которой являются технологии:

– облачных вычислений,
– больших данных,
– мобильного широкополосного доступа,
– наложенных сервисов и
– интернета вещей.

Развитие третьей платформы уже сегодня меняет жизненный уклад людей, который создан технологиями на безе персональных компьютеров, архитектуре киент-сервер, локальным сетям связи и интернету.

Отмечается, что необходимость и возможность внедрения целого комплекса новых технологий, обеспечивающих информационное взаимодействие в рамках третьей платформы, стимулируется и поддерживается:

– масштабами цифровой вселенной;
– значением информационной инфраструктуры для конкурентоспособности государств,регионов, предприятий, организаций, семей и отдельных личностей;
– образованием инфокоммуникационных технологий за счет конвергенции базовых информационных технологий сохранения, распространения и обработки данных;
– достижениями в области электроники, фотоники и радиотехники.

Коломойцев В.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ВОЗМОЖНОСТЕЙ ТИПОВ МЕЖСЕТЕВЫХ ЭКРАНОВ

В современных экономических системах, в результате повсеместного использования вычислительных сетей остро стоит вопрос организации защиты обрабатываемой в них информации от угроз прослушивания, повреждения и подмены, а также предотвращения заражения оконечных узлов работающих в вычислительных сетях.

Организация защиты вычислительных сетей, является одной из ключевых частей области информационной безопасности. В процессе обеспечения защиты трафика и устройств входящих в состав вычислительных сетей, требуется учитывать специфику деятельности организаций которые используются вычислительные сети, а также решать смежные с процессом организации безопасности сетей задачи, такие как контроль за производительностью и надежностью, стоимостью создания и обслуживания и сложностью архитектурной реализации вычислительной сети.

Одним из основных элементов обеспечения информационной безопасности сетей являются межсетевые экраны (МЭ). В зависимости от выбранного типа МЭ (или их набора) становится возможным решить требуемые задачи обеспечения защиты курсирующей по сети информации и защиты оконечных узлов сети от угроз извне.

В данной работе проведен анализ существующих групп МЭ – МЭ с фильтрацией пакетов, МЭ с адаптивной проверкой пакетов и МЭ прикладного уровня. Исследованы их возможности в вопросе обеспечения информационной безопасности, а также ограничения, налагаемые на процесс работы с информацией и с самой вычислительной сетью при использовании каждой из них в конкретной вычислительной сети. В зависимости от типа МЭ применяемого в вычислительной сети, влияние МЭ на различные ее аспекты (безопасность, производительность, надежность и т.д.) может разниться от несущественного и вплоть критически влияющего на сам процесс работы с сетью.

Выявлено, что наименьшее влияние на вычислительную сеть оказывают МЭ с фильтрацией пакетов (МЭ-Ф). Они являются одним самых распространенных типов МЭ и их применение практически никак не сказывается на производительности вычислительной сети. Также они позволяют наиболее легким способом разграничить области доступа узлов в сети, в связи со сравнительно малой себестоимостью и простотой своей настройки. Однако, в то же время, данный тип МЭ обеспечивает наименьший уровень безопасности вычислительной сети, т.к. не имеет возможности проверять содержимое и параметры проходящих по сети пакетов.

МЭ с адаптивной проверкой пакетов (МЭ-А) позволяют существенно повысить уровень сетевой безопасности в применяемой их организации. Данный тип МЭ способен подробно и тщательно анализировать содержимое проходящих через них пакетов, а также корректность их параметров. На рынке данный тип МЭ имеет широкое представление, что позволяет выбрать МЭ именно с теми параметрами и возможностями, которые необходимы для какой бы то ни было конкретной организации.

Негативными аспектами применения данного типа МЭ являются их высокая стоимость, возможная сложность настройки и слежения за правильностью установленных параметров, а также (в зависимости от «глубины проверки» пакетов) снижение производительности вычислительной сети. В

связи с этим применение данного типа МЭ (с максимально предоставляемыми ими возможностями) желательно на участках сети, где требуется обеспечить высокий уровень безопасности.

МЭ прикладного уровня (МЭ-П), также как и МЭ-А, способны анализировать содержимое пакетов. Ключевой стороной данного типа МЭ является то, что их можно установить на любое оконечный узел или вычислительное устройство и, в зависимости от имеющихся вычислительных мощностей устройства и установленных настроек МЭ, он будет способен обеспечивать защиту оконечного узла или же всей сети в целом на требуемом от него уровне.

Однако, их применение, имеет аналогичную негативную сторону, как и у МЭ-А – снижение производительности сети, в зависимости от «глубины проверки» пакетов. В связи с тем, что МЭ данного типа работают только на высоких уровнях сетевой модели OSI, то такие МЭ имеют ряд ограничений по скорости своей работы и анализу курсирующих по сети пакетов. При этом, благодаря тому, что их можно устанавливать на каждое отдельное вычислительное устройство, с настройкой строго под нужды этого устройства (или сегмента сети, к которому оно подсоединено), то это позволяет создавать более гибкие архитектурные решения вычислительной сети, тем самым балансируя нагрузку уже по вычислительным узлам, а не по участкам сети.

Применение любой из указанных групп МЭ, позволяет существенно повысить сетевую безопасность организации (или ее участков). Наиболее верным решением будет использование каждой отдельной группы МЭ наряду с другой, получая больший выигрыш от их положительных сторон и минимизируя влияние их негативных сторон.

Коршунов И.Л., Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННОГО ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ФОРМИРОВАНИЯ И РАСПРЕДЕЛЕНИЯ НАГРУЗКИ ВУЗа

Основным направлениям деятельности учебного отдела ВУЗа компании являются ежегодное планирование учебной работы в соответствии с руководящими документами и контроль за ее реализацией, которое предполагает, в том числе, выполнение массы рутинных операций, связанных с анализом учебных программ и формирования на их основе руководящих документов, определяющих учебную для деканатов, кафедр и ППС, а также - отчетных документов по ее реализации для планово-финансового управления.

Очевидно, что эффективность этой деятельности определяется как качеством разрабатываемых документов, так и их своевременной подготовкой в сжатые, как правило, сроки. Кроме этого остро стоит вопрос и о безопасности этих сведений, которые носят экономический характер. В этой связи автоматизация основных операций, связанных с процессом формирования и распределения учебной нагрузки в ВУЗе, которая существенно сокращает время на их выполнение и защита сведений о них, является жизненно необходимым условием успешной работа учебного отдела, деканатов и кафедр.

В настоящее время сотрудники учебного отдела для формирования соответствующих документов, используют программное обеспечение электронных таблиц пакета Microsoft Office. Действительно данная мера частично решает задачу по автоматизации основных расчетных операций, связанных с определением нагрузки и ее распределения по подразделениям.

Однако в этом случае остаются нерешенными масса проблем с вводом, синхронной обработкой данных, их передачей, а самое главное - сохранением целостности и безопасности структур этих данных. Поэтому временные затраты на указанные операции остаются достаточно большими, достоверность данных требует частого согласования, проверки и корректуры, а возможности реализовать их защиту достаточно слабые.

Современным направлением решения подобных задач является создание на базе инфокоммуникационных технологий автоматизированных информационных систем, которые смогут обеспечить оперативный доступ к необходимым информационным ресурсам в части требований руководящих документов. Программные комплексы подобных систем, как правило, основаны на использовании технологий баз данных и имеют клиент-серверную архитектуру, что и позволяет устранить недостатки простых «офисно-файловых» вариантов автоматизации и обеспечить требуемый уровень защиты данных.

Таким образом, для повышения эффективности деятельности учебного отдела, качества и безопасности, выполняемых им работ, следует ставить задачу на создание защищенного программного комплекса для формирования и распределения учебной нагрузки ВУЗа.

Нам представляется, что такой ЗПК ФиРУН должен решать следующие основные задачи:

1) ввод и долговременное хранение данных, необходимых для планирования учебного процесса;

2) формирование руководящих и отчетных документов, определяющих:

– общую учебную нагрузку университета;
– частную учебную нагрузку деканатов и кафедр;

– индивидуальную учебную нагрузку ППС
– требуемую штатную численность ППС

3) возможность удаленного доступа к информационным ресурсам, обеспечивающим разработку и получение данных руководящих документов и их защиту.

Для решения поставленной задачи данный ПК должен обеспечить автоматизацию следующих функций:

– предоставление возможности контролируемого доступа к его информационным ресурсам для персонала УО, деканата и кафедр.

– предоставление пользователям единого интерфейса управления информационными ресурсами и отображения документов.

– обеспечение единой централизованной аутентификации пользователей и поддержка иерархии доступа с системой приоритетов и паролей.

Кстати, в интересах организации более жесткого контроля за доступом к системе и ограниченного (числом факультетов и кафедр) числом пользователей есть смысл остановиться на реализации данного комплекса ПО в обычном клиент-серверном варианте его архитектуры.

Подобные системы, на наш взгляд, могут представлять и определенный коммерческий интерес для других учреждений, которые решают задачи организации учебного процесса.

Левкин И.М., Левкина С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ИНФОРМАЦИОННАЯ СТРУКТУРА КОНКУРЕНТНОЙ ОБСТАНОВКИ

Под конкурентной обстановкой предложено понимать положение, обстоятельства, условия существования конкурирующих хозяйствующих субъектов в конкретных исторических условиях в тот или иной момент общественного развития. Основные элементы конкурентной обстановки делятся на две группы: элементы микро- и макросреды. К элементам микросреды относятся сам хозяйствующий субъект, потребители товаров или услуг хозяйствующего субъекта, поставщики сырья для хозяйствующего субъекта, конкуренты хозяйствующего субъекта и т.п. К элементам макросреды относятся демография, экономика, природа, научно-технический прогресс, политическая ситуация, культура и т.п. В зависимости от сложившихся значений параметров элементов конкурентной обстановки возможно формирование тех или иных экономических угроз.

Эффективное ведение конкурентной борьбы невозможно без глубокого знания и постоянного мониторинга конкурентной обстановки. Решение этой задачи предполагает своевременное получение информации об основных элементах микро- и макросреды хозяйствующего субъекта. Этому способствует знание о местах концентрации необходимой информации, порядку ее распространения, хранения и защиты, иными словами знание информационной структуры конкурентной обстановки.

Под информационной структурой конкурентной обстановки предлагается понимать совокупность размещенных в географическом и информационном (электронном) пространствах узлах хранения информации об элементах обстановки (информационных узлах), связей между ними, а также средствах передачи, хранения и защиты информации.

К числу информационных узлов могут быть отнесены базы данных ПЭВМ, хранилища носителей информации в виде бумажных документов, магнитных, электронных и др. носителей (сейфы, специализированные библиотеки и т.п.), системы связи и передачи данных, одушевленные носители информации (действующие и бывшие сотрудники хозяйствующего субъекта, сотрудники аффилированных с хозяйствующим субъектом структур и т.п.).

Размещение информационных узлов в географическом пространстве определяется структурой хозяйствующего субъекта и его партнеров, динамикой их перемещения в пространстве и времени.

Размещение информационных узлов в информационном пространстве определяется выбранным способом обмена информацией в сети Internet(адресами размещенных контентов).

Основными особенностями информационной структуры конкурентной обстановки являются: относительная стабильность; наличие явных, скрытых и виртуальных информационных узлов; дублирование информации в информационных узлах электронного пространства, микширование оперативно важной информации, ее размытость по этим узлам и, соответственно, значительное число мелких информационных узлов.

Представление информационной структуры конкурентной обстановки в предлагаемом виде позволяет решить задачу рационального распределения сил и средств добывания информации деловой разведки по ее наиболее важным информационным элементам.

Лобанов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

АНАЛИЗ РИСКОВ ВЫПОЛНЕНИЯ ПОРТФЕЛЯ ЗАКАЗОВ НА ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

В докладе обосновывается идентификация типов рисков, в соответствии с критерием и ограничениями, предусмотренными математической моделью планирования выполнения комплекса задач. Анализируются методические подходы к количественной оценке рисков выполнения плана. Обосновываются рекомендации по управлению рисками.

В соответствии с критерием и ограничениями, предусмотренными планом выполнения комплекса бизнес-процессов предприятий информатизации, могут быть идентифицированы следующие типы рисков:

– отклонение планируемого общего финансового результата в меньшую сторону;

– потеря эффективности отдельно взятого бизнес-процесса, соответствующего заказанному проекту;

– потеря требуемой абсолютной ликвидности предприятия информатизации, т.е. сокращение сальдо накопленных денежных средств на расчетном счете ниже заданного значения;

– превышение суммарной допустимой трудоемкости по видам работ при выполнении комплекса бизнес-процессов в планируемом периоде;

– нарушение договорных сроков выполнения бизнес-процессов, соответствующих заказанным проектам.

Количественная оценка идентифицированных рисков может быть выполнена несколькими методами, в том числе анализом чувствительности, сценарным подходом, построением дерева решений, изменением денежного потока, имитационным моделированием. В докладе рассматривается подход к оценке проектных рисков на основе построения стохастической модели формирования портфеля заказов на проектирование информационных систем предприятия информатизации.

Для уменьшения влияния нежелательных факторов на порядок выполнения бизнес-процессов, выделенных в рамках планирования, предлагаются следующие рекомендации:

– совершенствование нормативной базы выполнения комплекса бизнес-процессов предприятия информатизации;

– сбор статистики, характеризующей нарушения показателей выполнения плана (по инцидентам и проблемам);

– увеличение стоимости выполнения комплекса работ по сравнению с расчетным показателем;

– увеличение по сравнению с расчетными сроков выполнения бизнес-процессов, соответствующих заказам клиентов;

– использование предоплаты для заказчика;

– утверждение графика платежей и включения его в договор в качестве приложения.

Минаков В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БАНКОВ

В условиях осложнения условий финансовой деятельности отечественных банков, в значительной степени лишенных доступа к дешевым денежным средствам на мировых рынках, прибыль существенно зависит от использования новых, особенно инновационных, банковских технологий. В их основе – конвергенция информационных технологий с банковскими. Получили развитие банковские продукты, базирующиеся на информационно-телекоммуникационных технологиях дистанционного обслуживания. Для юридических лиц предлагаются системы клиент-банк. Обслуживание таких клиентов полностью основано на использовании программных комплексов и систем телекоммуникаций. Для физических лиц банками предлагаются линейки продуктов на базе пластиковых карт: от дебетовых до кредитных. Интернет–банки, SMS–информирование, мобильный банк, системы виртуальных счетов, цифровые наличные, электронные платежные банковские, небанковские и интегрированные системы и т.п.

Очевидно, что повышение глубины проникновения перечисленных виртуальных систем повышает число угроз и вероятность компьютерных преступлений в банковской системе. Актуальной, следовательно, является проблема обеспечения адекватной системы превентивного предотвращения, локализации угроз, а соответственно обеспечения информационно-экономической безопасности банков.

Задачей данной работы является разработка концептуальной модели информационно-экономической безопасности банковской деятельности. Отличительной особенностью предлагаемой модели является переход от прямого противопоставления угрозам информационно-экономической безопасности таких средств, которые максимально снижают экономический ущерб банков, как это

делается в настоящее время, к системе, в структуру которой входят следующие элементы. Во-первых, блок угроз и опасностей дополняется учетом источников, их особенностей и свойств. Во-вторых к ним добавляется выявление сфер, из которых исходят опасности и угрозы. Принципиально важным, на наш взгляд, является декомпозиция объектов информационно-экономической безопасности банков на персонал, информационные ресурсы, материальные и финансовые ресурсы. В-третьих, выделяется блок направлений деятельности и мероприятий обеспечения безопасности, в рамках которых определяется спектр научно обоснованных методов, и только на их основе – выбор средств информационно-экономической безопасности.

Рассмотрим эффекты от использования предложенной структуры системы информационно-экономической безопасности банков. Учет сфер и источников угроз и опасностей позволяет оценить новые потенциально возможные инциденты за счет выявления ранее не проявлявшихся опасностей. Для этого, на наш взгляд, целесообразно выполнять аудит и превентивную оценку уровней зрелости информационных ресурсов смежных предприятий, которые являются контрагентами при осуществлении бизнес-процессов рассматриваемой кредитной организации. Действительно, любое нарушение в их информационной инфраструктуре может привести к нарушению в потоках информации. А ведь именно они определяют работу дистанционных систем банковского обслуживания. В это связи важно учитывать как технологический уровень информационно-телекоммуникационных систем контрагентов, так и подверженность воздействию рисков политического и иного характера. Нарушения в работе международной платежной системы Visав 2014 году из-за блокирования транзакций процессинговыми подразделениями, расположенными на территории США, привели к существенным потерям ряда банков, а также физических лиц на территории России.

Из предложенной концептуальной модели информационно-экономической безопасности следует, что такие прецеденты не могут быть предотвращены только инженерно-техническими средствами. Они требуют разработки и реализации мер системного характера. Назовем только некоторые из них. Во-первых, потребовались изменение правового обеспечения, в частности, принятие поправок в законодательство национальной системе платежных карт, о персональных данных в части их хранения на территории РФ и т.д. Во-вторых, принципиальное значение приобрел переход на отечественные технологические решения, а также создание отечественной информационно-технологической инфраструктуры процессинга, методов страхования финансовых ресурсов (обеспечение залоговым капиталом) и многое другое.

Таким образом, предложенная концептуальная модель информационно-экономической безопасности в банковской системе обеспечивает исчерпывающий охват и синхронизацию не только инженерно-технических средств, но выбор эффективных методов, а также необходимый и достаточный объем мероприятий по направлениям обеспечения такой безопасности.

Муравьев Е.В., Планкова М.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

АНАЛИЗ ПРИМЕНЕНИЯ SECAAS ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА

В современном мире, в условиях высокого уровня информатизации общества, вопросы обеспечения информационной безопасности играют важную роль, в связи с этим задачи, связанные с безопасностью образовательных и других государственных учреждений с каждым годом становятся все актуальнее. Поэтому внедрение информационных технологий, обеспечивающих безопасность, в сфере деятельности учебных заведений очень важно. В данном докладе мы рассмотрим перспективы и возможности применения SecaaS(Securityas a Service) технологий в вузе.

В любом вузе в наше время хранится и обрабатывается огромное количество информации и данных в электронном виде: от конфиденциальной информации о сотрудниках и студентах, данных об обеспечении учебно-методического процесса, до научно-исследовательских разработок и проектов в различных сферах деятельности, а также коммерческая, служебная и прочая, в том числе, конфиденциальная информация.

Вуз – это место повышенной активности как технически-грамотныхстудентов так и технически-неграмотных студентов и преподавателей, способных представлять угрозу для информационной безопасности. При проявлении угрозы важно быстроопределить источник, а так как аудитория пользователей информационной среды вуза непостоянна – это сделать очень сложно - в этом и заключается обоснование применения нестандартных методов обеспечения комплексной информационной безопасности в вузе.Которая включает в себя ограничения и авторизованный доступ к информации и данным на серверах учебного заведения и передаваемым через системы дистанционного обучения. В широком смысле данный термин включает в себясистему защиты интеллектуальной собственности вуза от внешних и внутренних агрессивных воздействий и систему управления доступом к информации и защиты от агрессивных информационных пространств[1].

Обеспечение защиты информации и информационных ресурсов, во время высокого уровня развития неконтролируемых интернет-сообществ и организаций, особенно актуально.

Внутренние серверы вуза от веб-угроз чаще всего защищают такие инструменты безопасности, как межсетевые экраны, серверы VPN, системы IDS/IPS. Трафик же конечных пользователей, как правило, может быть легко инфицирован. Вузы вкладывают слишком мало средств и сил в обеспечение инспектирования трафика, инициированного самими студентами и сотрудниками.Недостаток аппаратных мощностей и невысокое финансирование данной сферы деятельности в вузе, не позволяют использовать полнофункциональные инструменты защиты информации.

В противовес классическим способам обеспечения информационной безопасности конечных пользователей, на рынке появилась иная модель управления защитой организации. Это (Securityas a Service, SECaaS) – бизнес-модель управления безопасностью предприятия, являющаяся сегментом рынка SaaS.

SECaaS, по своей сути, - это перевод антивирусов, спам-фильтров и другого ПО, направленного на обеспечение безопасности, на аутсорсинг провайдеру, либо в частное «облако» организации, в нашем случае ВУЗа. Но этот термин может также обозначать менеджмент внутренней безопасности предприятия, осуществляемый подрядной организацией. Образование в России, в том числе и высшее, находиться в активном процессе взаимодействия со современной средой информационного общества, с новыми социально-политическим условиямии ограничениями, в том числе и экономическими. Снижение затрат, завязанных на содержании и обслуживании программно-аппаратного комплекса ВУЗа, а также на заработной плате сотрудников отвечающих за безопасность информационной среды внутри учебного заведения, в данных условиях не только выгодно, но и позволяет добиться большей гибкости в принятии управленческих решений.

Схема предоставления подобных услуг довольно проста. Весь вузовский трафик полностью переадресуется в «облако», где, на основе актуальных баз данных вирусных лабораторий, проходит фильтрацию. Исчезает необходимость приобретать и устанавливать какое-либо «тяжёлое» ПО на рабочие станции в корпусах учебного заведения.

Набор функций, которые можно отдать на «аутсорсинг» довольно внушительный. Однако, несмотря на очевидный прогресс в развитии рынка услуг информационной безопасности, многие вузы не готовы полностью отдавать такой стратегически важный аспект функционирования на аутсорсинг. Для перехода на такую модель обеспечения информационной безопасности требуется безоговорочное доверие стороне-провайдеру услуг и хорошо проработанная законодательная база, способная пресечь любое посягательство на кражу и использование информации проходящей через «облачные» каналы.

Николаев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ЗАДАЧИ УПРАВЛЕНИЯ ИНФОМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА

Системы условного доступа (ConditionalAccessSystems) – 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.

Основное требование к CAS-системам — надёжность работы. Сбои в работе или ошибки в программной части CAS чаще всего приводят к потере доступа к просмотру каналов абонентами, что негативно сказывается как на коммерческой составляющей, так и на имидже конкретной CAS-системы.

При эксплуатации CAS-систем требуется уделять особое внимание информационным рискам, т.к. их реализация, как упоминалось выше, будет иметь тяжелые последствия. Для управления информационными рисками CAS-систем требуется решить ряд задач:

1. Определение и локализация рисков;
2. Оценка последствий реализации риска;
3. Нормирование затрат ресурсов на текущие и аварийные работы;
4. Оптимизация распределения затрат на обслуживание.

В целом риски для CAS-систем очень похожи на риски других Информационных Систем, однако для CAS важность отдельных причин и факторов риска может серьезно варьироваться в зависимости от системы. Поэтому при решении первой задачи требуется обязательно учитывать специфику конкретной CAS-системы.

Последствия реализации рисков зависят от того, было ли нарушено функционирование основной услуги (доступ к просмотру каналов), количества пострадавших абонентов и длительности сбоя. Если работоспособность основного сервиса проверить несложно, то число пострадавших абонентов и длительность сбоя потребуют нечёткой оценки.

Хотя CAS-системы используются на протяжении длительного времени еще не сложилась единая практика оценки трудовых и материальных затрат на текущее обслуживание и устранение

сбоев в работе. От части, это объясняется сложностью данного класса систем и уникальностью каждого представителя семейства CAS.

Из всего вышесказанного можно сделать вывод, что управление информационными рисками систем условного доступа — важный процесс, а составляющие его задачи требуют применения мягких вычислений и экспертных оценок.

Омельян А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ СКРЫТОЙ МАРКИРОВКИ ОБЪЕКТОВ ПРИ ПОМОЩИ RFID-МЕТОК

В докладе рассматриваются достоинства радиочастотной идентификации.

Бесконтактная технология считывания информации позволяет производить скрытно как процесс маркировки объектов, так и процесс идентификации и контроля передвижения объекта. Технология обеспечивает высокую скорость идентификации. Объем памяти метки позволяет хранить не только идентификационный номер, но и другую информацию.

Проблемы использования RFID-метокносят организационный и технический характер. Реализации RFID-проектов в различных областях, таких как управление производством, охранные системы, учет и контроль, транспорт, простые платежные системы и др.прежде всего связаны с отсутствием стандартов в этой области. В настоящее время ведутся разработки национальных стандартов, регламентирующих уникальную идентификацию радиочастотной метки.

Кроме того до конца не разработана общая архитектура систем радиочастотной идентификации и параметры радиоинтерфейса RFID-системы для различных частотных диапазонов.

Проблемы также касаются построения архитектуры радиочастотной идентификации для скрытого и открытого контроля за объектами и архитектуры для управления объектами.

Приведенные в докладе достоинства радиочастотной идентификации,свидетельствующие о ее быстром развитии позволяют сделать вывод о том, что RFID-технология - этотехнология ближайшего будущего.

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

БЕЗОПАСНОСТЬ СИСТЕМ МНОЖЕСТВЕННОГО ДОСТУПА ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Доклад посвящен изучению аспекта безопасности систем множественного доступа для интернета вещей. В докладе рассматривается вопрос важности защиты на уровне устройств и приложений, а также вопрос важности защиты на уровне данных.Интернет вещей все еще является новым понятием, и немногие работники компаний знакомы с ним, а также понимают, что при работе с подобными системами способы сбора, обработки, хранения и передачи данных отличаются от привычных. Именно поэтому многие привычные техники обеспечения безопасности просто неэффективны. Существует множество промежуточных точек, в которых данные могут быть перехвачены. При этом большинство устройств интернета вещей не обладают достаточными вычислительными мощностями для реализации надежных алгоритмов криптографии. Как правило, в подобных сетях используются шлюзы и прокси, которые и являются объектами атак. Обеспечение безопасности связано здесь с защитой взаимодействий различных элементов связанной системы.

В докладе показано, что несмотря на все сложности с обеспечением безопасности, интернет вещей открывает значительные перспективы для развития технологий и новые возможности для бизнеса.

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОРГАНИЗАЦИЯ МЕТАДАНЫХ ДЛЯ БЕЗОПАСНОЙ СИСТЕМЫ ДЛИТЕЛЬНОГО ХРАНЕНИЯ

Доклад посвящен анализу организации метаданных в системах длительного хранения. Система длительного хранения данных служит для хранения различных видов информации на срок от 1 и до 100 и более лет. Потребителями такой системы могут быть как физические лица, по запросу которых система хранит фотографии, видео, документы и прочие данные, так и юридические лица, для которых важно безопасно хранить архивные данные. Для осуществления возможности поиска в системе длительного хранения необходимо использовать информацию о данных, содержащихся в системе, т.е. метаданные. Без них нельзя преобразовать цифровые данные (материальный уровень) в аналоговые, т.е. в смысловые (идеальный уровень). Кроме того, метаданные – это информация о расположении данных в пространстве, времени, привязанность к пользователю, местоположение на носителе (координаты пространства внутри носителя). Метаданные формируются в процессе сохранения информации, а также предполагают постоянное управление ими.

Предлагается классификация метаданных по следующим признакам:

по функциональным характеристикам:

– первичные (как правило заявленные инициатором хранения);

– технические (включающие в себя характеристики файлов с данными и характеристики носителя информации);

– адресные (включающие в себя адрес файла на носителе и адрес носителя в хранилище).

по необходимости формирования:

– обязательные (необходимые для идентификации и чтения информации);

– желательные (заявленные инициатором хранения).

– по месту хранения:

– хранимые на носителе вместе с информацией;

– хранимые в базе метаданных.

Предлагается алгоритм формирования метаданных на каждом этапе создания системы длительного хранения.

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

НЕРЕЛЯЦИОННЫЕ БАЗЫ БОЛЬШИХ ДАННЫХ

Доклад посвящен анализу использования нереляционных баз данных при хранении большого количества информации.

Количество хранимой информации постоянно растет, соответственно растут и требования к системам хранения данных. В связи с этим возникают новые задачи, связанные с хранением и работой с большими данными в таких системах. При постоянно возрастающем объеме данных традиционно использующиеся реляционные структуры теряют эффективность, следовательно, возникает необходимость использовать альтернативные структуры, то есть нереляционные базы данных.

Характеристика минереляционных баз данных являются:

– возможность работы с кластерами, что позволяет свободно наращивать аппаратные ресурсы системы хранения;

– работа без схемы, позволяющая свободно добавлять поля в базу данных без предварительного изменения её структуры, что обеспечивает гибкость базы данных;

– работа с агрегатными данными;

– как правило нереляционные СУБД – это системы с открытым исходным кодом.

Показано, что для обработки больших данных нереляционные СУБД являются более эффективными, поскольку время обработки запросов меньше, чем в реляционных. Однако реляционные структуры являются традиционными и имеют ряд неоспоримых достоинств, например, широкий спектр возможных запросов.

Показано, что в идеальном случае целесообразно использовать модель базы данных, содержащую как реляционные, так и нереляционные компоненты, т.е. некую комбинированную структуру.

Свеженцев И.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

О СОВЕРШЕНСТВОВАНИИ ЗАЩИТЫ ДОСТУПА К ИНФОРМАЦИИ О ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Доклад посвящен анализу путей совершенствования технологий, обеспечивающих защиту информации на предприятиях.

Рассматривается проблемная область систем контроля идентификации пользователей. За основу выбрана методика определения человека по клавиатурному почерку, который является уникальным.

Метод выбран в силу экономической ситуации, которая не предполагает больших объемов затрат на создание дорогих биометрическихустройств.

Актуальность проблемы обусловлена необходимостью создания современных систем проверки пользователей, которыеимеютдоступк носителям информации, относящейся к коммерческой тайне.

Рассматриваются основные принципы их построения и особенности функционирования.

Представлены логические блок-схемы функционирования и алгоритмы взаимодействия, описана структура базы данных, модули и потоки данных между ними, предлагается интерфейс пользователя и модель обоснованияразработки с использованием экономическихкритериев.

В процессепроектирования проанализированы научные публикации по указанной тематике, а такжефункционирующиесистемы подобного класса. Разработанный программный продукт позволяет на более высоком уровне ограничить доступ к закрытой информации, не имеющих на это прав пользователей.

Тестирование показало достаточную надежность и эффективность разработки.

Предполагается, что в дальнейшем будет продолжено ее совершенствование на основе современной операционной системы Windows 10.

Соколов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ОЦЕНКА УПРАВЛЕНЧЕСКОЙ ГИБКОСТИ В ПРОЦЕССЕ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ С УЧЕТОМ РИСКА И НЕОПРЕДЕЛЕННОСТИ

В докладе рекомендуется подход к оценке управленческой гибкости в процессе проектирования информационных систем (ИС) с использованием расширенного показателя чистой приведенной стоимости проекта, основанного на использовании реальных опционов.

Рассматриваются предпосылки целесообразности использования реальных опционов в управлении проектированием ИС как разновидности инвестиционного проектирования. К этим предпосылкам относятся, с одной стороны, наличие факторов риска и неопределенности в длительном процессе проектирования и, с другой стороны, возможности проявления управленческой гибкости менеджером проекта. В качестве основных факторов неопределенности и риска рассматриваются функциональность ИС, требования к которой первоначально заказчиком формулируется достаточно приблизительно и подлежат обоснованному уточнению на всех стадиях проектирования в соответствии с изменяющимися обстоятельствами, а также возможности финансирования проекта.

Методы оценки реальных опционов, такие как модель Блэка-Шольца, бинарного дерева и др., требуют использования исходных данных, которые трудно, а в ряде случаев невозможно получить в процессе проектирования ИС промышленных предприятий из-за недостаточности статистических данных, характеризующих денежные потоки данных проектов. К тому же эти модели не учитывают особенности проектирования ИС, которые могут быть отражены в опцион-ном подходе к проектированию.

Анализируются особенности опционного подхода в проектировании ИС, сведенные в четыре группы: 1. Наличие факторов неопределенности и риска, характерных для проектирования ИС; 2. Вариантный подход в проектировании; 3. Стадийность процесса проектирования ИС; 4. Итерационный характер процесса проектирования ИС. Предлагается классификация видов реальных опционов в процессе проектирования. Анализируются факторы управленческой гибкости по стадиям проектирования и видам реальных опционов.

Предлагается последовательная оценка экономической эффективности ИС на основе ожидаемых значений расширенной чистой приведённой стоимости проекта, уточняемых при переходе от одной стадии к другой.

Предлагается формула оценки управленческой гибкости, проявляющейся в использовании реального опциона для бинарного развития процесса проектирования.

Применение реальных опционов в процессе проектирования ИС с учетом особенностей этого процесса позволяет повысить оценку экономической эффективности проекта и его привлекательность.

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

БЕЗОПАСНОСТЬ СИСТЕМЫ УМНЫХ ВЕЩЕЙ

Доклад посвящен изучению аспекта безопасности в системе умных вещей. Рассматриваются технологии и надежность различных разработок, а также их ценовые показатели. Показано, что на рынке в последнее время появляется все больше предложений по внедрению систем безопасности для интернета вещей, так как умные вещи и их системы находят все большее количество внедрений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Устинов И.А., Виноградов А.А.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»

НОВЫЕ ВЫЗОВЫ ОТЕЧЕСТВЕННЫМ ТЕХНОЛОГИЯМ АВТОМАТИЗАЦИИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

В докладе анализируются новые вызовы в области технологий создания отечественных систем управления критическими инфраструктурами государственного, хозяйственного и военного назначения. В связи с повсеместной информатизацией всех областей деятельности на базе импортных компьютеров и с внедрением новых глобальных технологий кибер-атак серьёзно возросли риски масштабных информационных вторжений в работу критически важных систем со стороны враждебных стран. Ключевые задачи импортозамещения состоят не в копировании импортной техники, а в создании отечественных информационных услуг, средств и систем на принципах, алгоритмически и технологически способных противостоятьсовременным методами и средствамкибер-агрессии.

Геополитическое противостояние переместилось в область информационных технологий. Дистанция технологического отставания России от стран Запада является основным инструментом сдерживания, который не даёт России достичь стратегического превосходства в области информационных технологий. В этих условиях необходимо жёстко руководствоваться принципом разумной функциональной достаточности, который позволяет создавать системы с максимально отечественной глубиной происхождения при полной реализации требуемого функционала.

В докладе обсуждаются основные подходы к реализации принципа разумной функциональной достаточности в отечественных алгоритмах, аппаратуре и в программном обеспечении. Обоснована необходимость дальнейшего развития опыта АО «НПО «Импульс» по созданию уникальной школы специалистов по разработке эффективных систем на базе технических отечественных средств с ограниченными функциональными характеристиками.

Созданные универсальные отечественные технические средства и программное обеспечение должны стать доступными для разработчиков отечественных систем. Необходимо заботиться не только о самих системах, но и об отечественных технологиях обеспечения их жизненного цикла на этапах разработки, изготовления, отладки, испытаний и эксплуатации.

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

ТЕХНОЛОГИИ МИНИМИЗАЦИИ ИЗБЫТОЧНОСТИ ПРИ МОНИТОРИНГЕ И УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ОБЪЕКТОВ

Анализ и синтез средств и систем обеспечения информационной безопасности (ИБ) критических объектов, включая объекты морской техники и морской инфраструктуры (ОМТИ), в свете комплекса требований государственных, ведомственных и корпоративных регламентов по широкому спектру специализаций предусматривает объективную качественную и количественную оценку уровня ИБ критических объектов. А также последующий анализ и синтез концептуальных и технологических решений по обеспечению современных требований к ИБ ОМТИ. В условиях решения национальной задачи обеспечения конкурентной способности и имортозамещаемости разрабатываемых технологий и систем обеспечения ИБ (СОИБ), это требование становится особенно актуальным и востребованным. И, прежде всего, в интересах концентрации национальных средств и компетенций специалистов при решении методологически и технологически сложных задач обеспечения защищенности современных систем автоматизации, противоборства в информационной сфере.

Среди комплекса решаемых при этом задач и проблем управления ИБ ОМТИ особое внимание, по нашему мнению, должно уделяться проблеме и технологиям минимизации избыточности, и, в первую очередь, информационной избыточности так как её необоснованное наращивание приводит, как показывает ретроспективный анализ целого ряда технологических решений, к существенному снижению качества и эффективности СОИБ в следствие избыточности по характеристикам структурной, функциональной и конструктивной сложности, энергообеспечения и обеспечения робастности, эксплуатационной сложности, напряженности обслуживания и другим параметрам.

Именно оптимизация избыточности, как комплекса параметров и характеристик СОИБ, отражающих наличие в них возможностей и меру возможной минимизации (сокращения) возможностей по соответствующему критерию, превышающих необходимые для обеспечения их нормального функционирования, т.е. с заданными показателями достижения цели (своего целевого предназначения).

Обычно избыточность в технических системах, включая СОИБ, вводится для повышения устойчивости функционирования с учетом возможности изменения условий их применения, безусловно, отличающихся от среднестатистических данных, используемых, как правило, для задания уровня функциональной эффективности (проектного качества) СОИБ.

В общем случае нормирование избыточности достигается в процессе исследовательского проектирования путем поиска компромиссных технических решений, обеспечивающих минимизацию обобщенных затрат для реализации требуемого уровня их качества и устойчивости функционирования.

Частными видами информационно-технической избыточности (ИТС) являются: функциональная; информационная; алгоритмическая; аппаратная; техническая (временная, энергетическая и т.п.); ресурсная и другие. Как правило, представляется весьма сложным строго разделить избыточность по соответствующим видам вследствие сильной их причинно-следственной связи. В этой связи следует отметить то важное обстоятельство, что специалисты, ученые этой проблеме непрерывно уделяют внимание и целый ряд решений по оптимизации ИТС известны и имеют большое практическое значение. Традиционно ИТС, прежде всего, определяется избыточностью отсчетов при аналого-цифровом преобразовании данных. Этому направлению на сегодня за более, чем 100-летний период, уделено очень большое число исследований и достигнуты значительные результаты. Применительно к задачам обеспечения ИБ и, в первую очередь, критических объектов типа ОМТИ сегодня среди других особого внимания заслуживают следующие концептуальные и технологические решения:

– квалиметрического анализа, синтеза и оптимизации проектных и управленческих решений (технология АСОР, программные комплексы (ПК) поддержки – «КРОПУР» (2002 г.), «АСОР» (2007 г., «МКО-БЖКС», 2013 г.). Данные ПК именно в комплексе на основе оптимизации системотехнических характеристик СОИБ позволяют комплексно минимизировать их избыточность. В том числе при решении таких сложных организационно-технических задач, как борьба за живучесть корабля, судна (БЖКС);

– информационно-аналитической и интеллектуальной поддержки принятия управленческих решений (технология СИП ПУР, ПК «СИП ЛА-ГО о3», 2014 г., «МКО-ИБ», 2015 г.). Данные ПК на основе оптимизации принимаемых операторами организационно-технических решений по управлению СОИБ позволяют в комплексе «оператор-техника» минимизировать функциональную и ресурсную избыточность. В том числе за счет минимизации объёма и максимизации качества (ценности) визуализируемой информации, представляемой оператору, а также представления в максимально удобной для восприятия оператором форме ранжированных по ожидаемой эффективности (качеству) проектов управленческих решений, что позволяет снизить негативное влияние «человеческого фактора;

– минимизации структурно-функциональной и конструктивной избыточности пультов управления СОИБ на основе мобильных рабочих станций в защищенном исполнении типа смартфон, планшет на основе структурно-алгоритмической и функциональной оптимизации и кодирования данных.

Башкирцев А.С., Паращук И.Б.
Россия, Москва, в/ч 52686,
Санкт-Петербург, Военная академия связи имени Маршала Советского СоюзаС.М. Буденного

ОБОСНОВАНИЕ АКТУАЛЬНОСТИ ФОРМИРОВАНИЯ ПЕРСПЕКТИВНОЙ ЗАЩИЩЕННОЙ АВТОМАТИЗИОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СВЯЗЬЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В условиях обострения мировой геополитической обстановки актуальное значение приобретает необходимость решения проблемы по защите исторически-обусловленных интересов РФ различными способами, в том числе и способами вооруженного противоборства, как крайней меры. Существующие тенденции развития способов классического вооруженного противоборства переводят его в плоскость вооруженно-информационного противоборства, что обусловлено, прежде всего, ростом потенциальных возможностей «информационноемких», роботизированных видов вооружений и потребностью достижения информационного превосходства над противником. Данные факторы определяют увеличение требований к сокращению цикла управления и повышению устойчивости управления силами и средствами специального назначения (СиССН), что достигается применением современной технической основы системы управления и ее главной компоненты - системы связи.При этом, как и прежде, к основным задачам, возлагаемым на систему связи СиССНотносят доведение с заданными вероятностно-временными характеристиками директив и

сигналов, качественное и своевременное предоставление информационно-телекоммуникационных услуг; выполнения требований устойчивого, непрерывного, оперативного и скрытного управления, а также создание условий для обеспечения безопасности, достоверности и целостности информации.

Решение этих задач обеспечиваетсясистемой управлениясвязью СиССН, которая является подсистемой системы управления СиССН и включает в себя техническую основу управления связью, состоящей в свою очередь из защищенной автоматизированной системы управления связью (АСУС), телекоммуникационной служебной подсистемы и специальных систем контроля и обеспечения информационной безопасности системы связи СиССН.АСУС СиССН является основной технической инфраструктурой для обеспечения планирования, подготовкии применения сил и средств системы связи СиССН и в настоящее время характеризуется следующим состоянием:применение средств автоматизации управления связью носит ограниченный характер и не поддерживает выполнение основных и наиболее трудоёмких функций управления связью в СиССН;в существующих оперативно-технических требованиях к системе связи СиССН отсутствуют качественные и количественные требования к архитектуре системы, а так же нормы на показатели и параметры служб, способы обслуживания пользователей различных категорий и услуги информационного обеспечения в АСУС СиССН; комплексы автоматизации и обмена управляющими данными по связи для подсистемытехнологического управления являются уникальными, что приводит к отсутствиюунификации; отсутствует технологическая политика реализации дистанционного мониторинга и управления средствами связи; взаимодействие пунктов управления связью АСУС с пунктами управления ресурсами операторов ЕСЭ реализовано только на организационном уровне в неавтоматизированном режиме.

Таким образом, система управления связью нуждается в полноценной автоматизации, сейчас она не всегда отвечает требованиям. Именно поэтому актуальны задачи, направленные на повышение качества автоматизированной системы управления связью СиССН: выработку научнообоснованных решений; учет комплексного развития информационных, вычислительных и телекоммуникационных ресурсов системы управления связью СиССН; совершенствование нормативной и правовой базы, а также рациональное использованию бюджетных лимитов.

Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

К ВОПРОСУ ЗАЩИТЫ ЗАКРЫТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДНАЗНАЧЕННОГО НА ЭКСПОРТ

Цели защиты - предотвращение пиратского копирования и несанкционированного использования программ.

Обобщая недостатки систем защит от пиратства следует отметить следующие особенности:

– законный владелец должен иметь возможность устанавливать программу неограниченное количество раз и на любую конфигурацию компьютера;

– законному владельцу необходимо запретить (программно-аппаратными методами) передавать ПО 3-м лицам для использования;

– при получении ПО, третьи лица не могут воспользоваться программным обеспечением т.к. не являются законными владельцами.

Классическая схема защиты с помощью регистрационного ключа, вводимого один раз, как известно, скорее способствует распространению ПО, чем препятствует, если регистрационным ключом не является номер банковской карты. Проверять номер следует в разным местах и по частям. На любом этапе проверки программа прекращает работу, если введенный ключ оказался не верен. Так как банковская карточка у юридического лица использоваться не будет, то рассчитывать на сохранность регистрационного ключа нельзя. Возможно ввести систему сеансовых ключей. Т.е. при каждом новом запуске программа использует новый ключ. При перезаписи на новую машину будет считан, допустим, ключ №34, а не, №58, который бы должен был считаться на той машине, откуда был переписан оригинальный файл программы. Добиться этого можно, к примеру, путем сбрасывания тайного счетчика. Набор ключей, характерных для новой машины рассчитывается исходя из случайных параметров, которые для каждой новой установки ПО разные и соответственно один набор ключей соответствует только одной установке. Генератор ключей удобно реализовать в виде Web-приложения, при доступе к которому возможно удостовериться, что ключи обновляет именно владелец ПО. Каждый новый ключ имеет непосредственную зависимость от предшествующего ключа, чтобы только один из всех позволял работать программе в текущем сеансе.

Пользователь получает вместе с дистрибутивом нулевой ключ, необходимый для инсталляции. После ввода он хэшируется и суммируется с некоторым случайным числом. Полученное значение сохраняется и будет являться переменной x для функции преобразования F(x) в 1-ый сеансовый ключ (K1). Т.е. $F(x) = K1$, где $x = H(K0) + E(s)$. При этом K0 - это регистрационный номер, H – функция хэширования, а E – энтропии от s - состояния компьютера в случайный момент времени.

Дальнейший способ получения ключей основывается только на функциях F и H: K1 → H(K1) → F (H(K1)) → K2; K2 → H(K2) → F (H(K2)) → K3

От K1 рассчитываем хэш H(K1), от хэша – следующий ключ - K2. Таким образом у нас есть набор {K1 ,K2, K3}. Примерный алгоритм защиты следующий:

1) $H(K_1)$ – каким-то образом хранится в программе. Это может быть и внутренний массив, и внешнее хранилище.

2) при запуске программы считывается ключ K_2 и с помощью обратной функции к F получается хэш для сравнения: $Ф(K_2) = H(K_1)$;

3) сравнивается полученный хэш с записанным в программе ранее (см. шаг 1).

4) если они не совпадают, то осуществляется выход из программы, как нелегальной.

5) если же совпадают, то удаляется хэш-значение из области хранения, как уже использованное, и записывается на это место новый хэш, получаемый расчетом от K_3 : $Ф(K_3) = H(K_2)$ – тогда при следующем запуске будет производиться сравнение именно с ним.

6) увеличивается значение счетчика.

При таком подходе потенциальному взломщику трудно создать генератор сеансовых ключей т.к. он не знает в цепочке алгоритм хэширования и счетчика, которые, допустим можно выявить. Увеличение числа ключей сделает сложность взлома сравнима с со сложностью обнаружения этих участков в разных местах программы. Увеличение трудоемкости взлома можно добиться, если использовать для разных ключей отличные друг от друга счетчики и хэш-функции.

Использование части ключа в процессе работы защищаемой программы затруднит отключение такого механизма интегрированной защиты.

Для реализации описанных механизмов в разрабатываемых программах могут быть полезны лабораторные анализаторы качества кода и контроля программных закладок.

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

ПРИНЦИПЫ ПОСТРОЕНИЯ И АРХИТЕКТУРАРЕГИОНАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ «БЕЗОПАСНАЯ ТЕРРИТОРИЯ»

В последнее время в целях решения задач обеспечения безопасности жизнедеятельности населения во многих регионах страны по инициативе регионов, различных министерств и ведомств (МВД, ФСБ, МЧС) созданы и функционируют системы обеспечения безопасности и противодействия ЧС. Однако они создавались в различное время, разными ведомствами, построены по различным принципам, что усложняет их дальнейшую интеграцию в единую систему.

Сейчас в целях решения задач национальной обороны крайне актуальной стала задача создания единого регионального комплекса технических средств и информационно-аналитической системы обеспечения региональной безопасности - региональной системы безопасности «Безопасная территория», обеспечивающей объединение ведомственных систем безопасности на основе единых принципов, единой защищенной мультисервисной телекоммуникационной сети в единую региональную систему с последующим ее включением в инфраструктуру Региональных центров и Национального центра управления обороной страны.

В докладе рассматриваются принципы построения региональной системы безопасности «Безопасная территория», на примере МИТС КСОБЖН Ярославской области, обеспечивающей эффективное объединение ТС всех существующих региональных и ведомственных подсистем безопасности.

Кондратьев Д.А, Ипатов О.С.
Россия, Санкт-Петербург, ОАО «Концерн «Гранит-Электрон»,
Санкт-Петербургский политехнический университет Петра Великого

МЕТОДЫ СИНТЕЗА АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЦЕЛЕУКАЗАНИЯ И ОСВЕЩЕНИЯ ОБСТАНОВКИ НА БАЗЕ ДИСТАНЦИОННО-ПИЛОТИРУЕМЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Современный уровень науки и техники позволяет сделать комплексные системы мониторинга полностью автоматическими, но это связано с рядом трудностей, и сложностью перекрестного анализа поступающей информации, отвечающего за адекватность решения принимаемого системой и необходимостью обеспечения информационной безопасности. В настоящее время представляется возможным использовать автоматизированные экспертные системы.

Важным вопросом построения интеллектуальной системы целеуказания и освещения обстановки является разделение функций между оператором и комплексом управления. Если основной задачей вылета является эффективный мониторинг морской и наземной поверхности, то задачи оператора по выполнению пилотажных операций должны быть сведены к минимуму, тем самым максимизируя его внимание на работу с обзорными средствами, оценку обстановки и принятие решения. С другой стороны, передача оператору максимального количества функций по

управлению дистанционно-пилотируемым летательным аппаратомпозволяет использовать простейшие системы автоматизированного управления на борту дистанционно-пилотируемого летательного аппарата. Компромиссным решением может быть передача наземному вычислителю максимально возможной доли вычислений, связанных с формированием законов управления, и ограничение функций бортового оборудования отработкой команд, передаваемых по телеметрической линии связи.

Эргатическая надежность достигается повышением информационной безопасности системы путем использования синтеза алгоритмов управления. При проектировании разрабатываемой системы целеуказания и освещения обстановки удовлетворяющей требованиям эффективности и информационной безопасности, проводится структурный и параметрический синтез информационно-алгоритмического обеспечения.

Таким образом, разработка адекватных математических моделей, параметрический и структурный синтез алгоритмов работы аппаратуры управления, внедрение интеллектуальных алгоритмов обработки информации в интеллектуальные системы мониторинга, повышают эффективность использования комплексов освещения обстановки и целеуказания.

Паращук И.Б., Ковальченко Д.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного

ОПРЕДЕЛЕНИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ ЗАЩИТЫИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХСПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В процессе активного развития работ по защите информации как в России, так и за рубежом наряду с разработками конкретных вопросов защиты формировались общеметодологические принципы (общие положения) построения и функционирования подсистем защиты информациипри взаимодействии телекоммуникационных сетей (ТКС) и автоматизированных систем специального назначения (АССН) с глобальной сетью Интернет. Соблюдение требований таких принципов в общем случае способствует повышению эффективности защиты. Примерно сформированная и активно обсуждаемая в современной специальной литературе система включает перечень общеметодологических принципов построения и функционирования подсистем защиты информации: концептуального единства, адекватности требованиям, гибкости (адаптируемости), функциональной самостоятельности, удобства использования, минимизации предоставляемых прав, полноты контроля, адекватности реагирования на угрозы и экономичности.

Концептуальное единство означает, что архитектура, технология, организация и обеспечение функционирования как подсистемы защиты информации в целом, так и составных ее компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции защиты информации.

Адекватность требованиям означает, что подсистема защиты информации должна строиться в строгом соответствии с требованиями к защите, которые в свою очередь определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

Гибкость (адаптируемость) подсистемы защиты означает такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры ТКС и АССН, технологических схем или условий функционирования каких-либо их компонентов.

Функциональная самостоятельность предполагает, что подсистема защиты информации должна быть самостоятельной обеспечивающей подсистемой ТКС и АССН и при осуществлении функций защиты не зависеть от других подсистем.

Удобство использования означает, что подсистема защиты не должна создавать дополнительных неудобств для пользователей и персонала ТКС и АССН.

Минимизация предоставляемых прав означает, что каждому пользователю и оператору должны представляться лишь те полномочия на доступ к ресурсам ТКС и АССН, которые ему действительно необходимы для выполнения своих функций.

Полнота контроля предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться подсистемой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.

Активность реагирования означает, что подсистема защиты информации должна реагировать на любые попытки несанкционированных действий – просить: повторить действие; задерживать выполнение запросов; отключать структурный элемент, с которого осуществлено несанкционированное действие; исключать нарушителя из числа зарегистрированных пользователей и подавать специальный сигнал.

Экономичность подсистемы защиты информации означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на подсистему защиты должны быть минимальными.

Присяжнюк А.С.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»

КОГНИТИВНАЯ РАДИОСЕТЬ НА БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТАХ ДЛЯ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ РЕГИОНА

Обеспечение безопасности жизнедеятельности региона в чрезвычайных ситуациях требует оперативной, живучей и безопасной радиосвязи для обеспечения эффективного взаимодействия заинтересованных структур управления.

Наиболее эффективно эта задача решается с помощью наложенной радиосети на беспилотных летательных аппаратах. Особенно это актуально в труднодоступных территориях, например, при пожарах , наводнениях, сходов лавин в горах и т.д.

Предлагается вариант построения широкодиапазонной пакетной радиосети построенной на когнитивных принципах с возможностью расположения базовой сети на мини беспилотниках организованных по схеме «РОЯ», т.е. группового применения.

Рассмотрена система управления развертывания и оперативным управлением «РОЕМ» беспилотников и радиосредств расположенных на них.

Приводятся сравнительные оценки эффективности наложенной сети с традиционными способами организации взаимодействия структур управления.

Ходаков В.Е., Соколова Н.А., Антипенко И.В., Бабина О.В.
Россия, Керчь, Керченский государственный морской технологический университет

ОЦЕНИВАНИЕ РАЗВИТИЯ ОДНОГО КЛАССА СЛОЖНЫХ СИСТЕМ

Среди множества сложных систем особое место занимают социально-экономические системы (СЭС), которые в свою очередь разделяются на СЭС разных уровней и типов. Самой сложной из них является современная цивилизация, как сложная, целеустремленная, территориальная, иерархически и организационно структурированная глобальная социально-экономическая метасистема.

Каждая СЭС характеризуется различными экологическими, географическими, природно-климатическими средами. Причём даже в пределах отдельных СЭС эти среды могут значительно отличаться друг от друга. Эти отличия могут формировать как разную ментальность социума, так и разный уровень развития экономики.

Одним из классов СЭС являются страны Восточной Европы, располагаемые в зоне более неблагоприятных природно-климатических условий, чем страны Западной Европы. Здесь производство и экономика характеризуются значительно большими издержками, большей себестоимостью продукции, меньшей эффективностью, более длительными сроками окупаемости .

Для повышения эффективности экономики, снижения уровня негативного влияния природно-климатических факторов необходимо иметь возможность выделять внутри территорий зоны, в которых производство характеризовалось бы минимальными издержками, для чего должна быть методология выбора территорий с учётом природно-климатических условий (факторов). Это в определённой степени аналогия для давно применяемой на примере северных стран методов выбора экономически активных зон.

Цель работы. Целью работы является разработка и изложение основных подходов методологии определения зон, отдельных территорий, наиболее подходящих для формирования зон ускоренного экономического развития.

Основное содержание работы. В основе методологии лежат процедуры оценивания, идентификации состояния СЭС.

Процессы управления развитием СЭС весьма динамичны, протекают достаточно противоречиво, что обуславливает необходимость мониторинга состояний и постоянной информационной поддержки управленческих решений. СЭС и их составные компоненты характеризуются пространственной и функциональной распределенностью, асинхронным взаимодействием процессов и компонент.

Изложена методология многофакторного оценивания одного класса социально-экологических систем – регионов с учётом природно-климатических условий для выбора экономически активных зон, где производство характеризуется минимальными значениями издержек. Для оценки состояния СЭС используется функционал обобщённого критерия построения ранжированного ряда [4-7]. Данная методология реализуется в программных продуктах для расчётов оценки инвестиционной привлекательности и устойчивого развития социально-экономических систем с учётом и без учёта влияния природно-климатических факторов.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ

Горшков Р.А., Минина М.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОСНОВНЫЕ ПРОБЛЕМЫ СТАНДАРТА БЕЗОПАСНОСТИ BLUETOOTH

К основным проблемам стандарта безопасности Bluetooth относятся:

– стойкость генератора псевдослучайной последовательности не определена: генератор может производить статические и периодические последовательности, которые могут уменьшить схему авторизации. Короткий PIN позволяет: Слабые PINs, которые используются для генерации ключа соединения и авторизации, могут быть легко подобраны. Повышение длины PIN существенно увеличивает безопасность соединения, но, как правило, пользователи используют короткие последовательности(1-4 символа);

– совершенного пути генерации и распределения PIN не существует: распределение PIN´ов в больших Bluetooth сетях с множеством пользователь – сложная организационно-техническая процедура;

– длина ключа шифрования недостаточна: BluetoothSIG нуждается в разработке более стойкой процедуры генерации ключа инициализации;

– единичный ключ повторно используется и становится общим после использования: единичный ключ – ключ соединения, который

– мастер-ключ общий: BluetoothSIG требует разработки лучшей схемы распространения ключей;

– не существует авторизации пользователя: обеспечивается только авторизация устройства. Должна применяться безопасность уровня приложений и авторизация пользователей;

– попытки авторизации не ограничены: BluetoothSIG нуждается в разработке ограничительного параметра для предотвращения неограниченного числа запросов. Спецификация Bluetooth требует создания тайм-аут периода между повторяющимися попытками, который должен увеличиваться экспоненциально;

– слабый алгоритм поточного шифрования E0: E0 произошел от поточного шифра с суммированием и комбинированием. Это был поточный, который был предложен Мэсси и Руппелом в середине 80х. Наиболее мощные атаки на это шифрование – корреляционные атаки с полным поиском в ограниченном пространстве ключей. Недавний результаты криптоанализа показали, что E0 шифрование слабее этого;

– недостаточная длина ключа: должно быть установлено международное соглашение о минимальной длине ключа;

– совместное использование ключа соединения может привести к подслушиванию: злоумышленник возможно может нарушить безопасность между 2 другими пользователями(получить неавторизированный доступ) если он имеет связь с любым из этих пользователей. Это происходить потому, что ключ соединения, полученный из информации общего пользования, незакрыт;

– конфиденциальность может быть нарушена, если адрес Bluetooth устройства перехвачен и связан с оборудованием злоумышленника: BD_ADDR связанный со злоумышленником, можут привести к несанкционированной регистрации, что вызовет потерю конфиденциальности;

– авторизация устройств – процедура, основанная на простом запросе-ответе общим ключом: односторонняя запрос-ответ авторизация – предмет атаки типа man-in-the-middle. Двухсторонняя авторизация требует обеспечения проверки подлинности пользователя и сети;

– End-to-end безопасность не выполняется: только индивидуальные линии связи зашифрованы и аутентифицированы. Информация дешифруется в промежуточных пунктах. Должно быть разработано прикладное ПО выше уровня Bluetooth ПО;

– службы безопасности ограничены: аудит, неотречение и другие службы не существуют.

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМЫ ПРОГНОЗИРОВАНИЯ КОСМИЧЕСКОЙ ПОГОДЫ

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.

Игнатьев М.Б., Ненашев В.А., Катермина Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения,
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 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 и Сахалина.

Кочкаров Л.С., Минина М.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ГИДРОГРАФИЯ И ГИДРОМЕТЕОРОЛОГИЯ КАК СОСТАВЛЯЮЩАЯ БЕЗОПАСНОСТИ МОРЕПЛАВАНИЯ

Роль гидрометеорологических прогнозов и изученность морского дна – важная составляющая в устойчивом развитии морского транспорта. Так как морской транспорт на сегодняшний день обслуживает 62% мирового грузооборота. Именно благодаря развитию морского транспорта океан уже не разделяет, а соединяет страны и континенты. Общая протяженность морских трасс составляет миллионы километров. Морские суда транспортируют главным образом массовые грузы: нефть, нефтепродукты, уголь, руду, зерно и другие, причем обычно на расстояние 8 — 10 тыс. км. "Контейнерная революция" на морском транспорте привела к быстрому росту перевозок и так называемых генеральных грузов — готовых изделий и полуфабрикатов. Морские перевозки обеспечиваются морским торговым флотом, общий тоннаж которого превышает 420 млн. т.

Также гидрографические и гидрометеорологические характеристики морских акваторий обязательно принимаются в расчет при разработке разных видов водной техники, эффективность которых зависит от этих характеристик.

В соответствии с Морской доктриной Российской Федерации на период до 2020 года одной из задач национальной морской политики на Арктическом направлении является обеспечение национальных интересов Российской Федерации в отношении Северного морского пути, централизованное государственное управление этой транспортной системой, ледокольное обслуживание и предоставление равноправного доступа заинтересованным перевозчикам, в том числе иностранным.

Малыгин Е.Ю., Митько В.Б.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОСНОВНЫЕ ПРИЧИНЫ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ

Сеть мобильной связи представляет собой сложную систему коллективного пользования, включающую в себя комплекс современных программно-технических средств по предоставлению комплекса услуг связи и передачи данных, эксплуатируемую специалистами различного профиля. Среди основных особенностей сети мобильной связи, обусловливающих наличие угроз информационной безопасности, следует отметить следующие:

– сеть связи является сложной информационной системой и, как любая информационная система, подвержена атакам злоумышленников на информационную сферу;

– сеть мобильной связи является публичной и обслуживает сотни тысяч, а наиболее крупные и миллионы пользователей. Этот факт создает объективную почву для появления субъектов со злонамеренными целями;

– сеть мобильной связи для предоставления широкого спектра услуг пользователям подключается к сетям связи общего пользования, включая междугороднюю и международную связь, к сетям поставщиков услуг и контента. Такие подключения увеличивают вероятность атак из внешних сетей;

– управление сетями связи третьего поколения осуществляется с помощью программно-технических средств, наиболее подверженных воздействию вредоносных программ. Успешная атака на систему управления может привести к существенным материальным потерям;

– сети связи 3G предоставляют пользователям широкий спектр услуг. Некоторые из них могут быть использованы злоумышленниками для нанесения ущерба как операторам связи, так и отдельным гражданам;

– мобильные терминалы в сетях 3G представляют собой мобильные компьютеры с общим и специальным программным обеспечением. С одной стороны, они являются объектом атак злоумышленников, а с другой – сами становятся источником угроз информационной безопасности.

Опыт эксплуатации сетей подвижной связи предыдущих поколений показывает, что угрозы имели место всегда, в той или иной степени приводя к нарушению информационной безопасности или не имея никаких последствий вследствие трудности реализации.

Митько А.В. , Порокин Д.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОСОБЕННОСТИ СЪЁМКИ РЕЛЬЕФА ДНА ДЛЯ СОЗДАНИЯ МОРСКИХ НАВИГАЦИОННЫХ КАРТ В ИНТЕРЕСАХ БЕЗОПАСНОСТИ МОРЕПЛАВАНИЯ

Современная гидрография во многом базируется на использовании достижений геоматики. За последние 10–15 лет методы выполнения гидрографических съемок претерпели радикальные изменения. Это связано с широким внедрением персональных компьютеров и новых технических средств, таких как спутниковая навигационная аппаратура (СНА) с обработкой фазы несущей, цифровых однолучевых (ОЛЭ) и многолучевых эхолотов (МЛЭ), гидролокаторов бокового обзора (ГБО), а также батиметрических гидролокаторов бокового обзора (БГБО). Появились инновационные гидрографические технологии в виде электронных гидрографических информационных систем (ЭГИС) различного назначения. В большинстве ЭГИС возможен прямой экспорт результатов съемки рельефа дна в обменный формат электронной навигационной карты (ЭНК) S-57, что существенно сокращает время доведения картографической информации до потребителя.

На сегодняшний день, основную информацию, необходимую для создания морских навигационных карт и пособий, предоставляет поле рельефа морского дна, исследуемое посредством промера. Съемки для этого вида гидрографической деятельности всегда являлись основными при выполнении гидрографических исследований. Для проведения съемки используются однолучевые и многолучевые эхолоты в сочетании с гидролокаторами бокового обзора. В наиболее мелководных районах (акватории портов, подходные каналы и фарватеры) вместо МЛЭ с успехом могут быть использованы эхотралы. Современная аппаратура, включая МЛЭ может быть размещена на небольших судах и катерах, что повышает экономическую эффективность съемок. Выполнение съемки регламентируется стандартом S-44 (редакция 5,2008) Подготовленным Международной Гидрографической Организацией (IHO). Результаты гидрографических работ, как правило, предоставляются в виде планшетов промера, а также в виде цифровой модели рельефа, построенного на основе файла точек (файл формата x,y,z). Вес цикл выполнения работ поддерживается какой-либо из доступных на рынке промышленных ЭГИС.

Основной тенденцией является импорт результатов промера непосредственно в формат базы данных S-57 с целью ускорения создания электронных навигационных карт. Данную опцию поддерживают такие ЭГИС, как «Hypack MAX», QINSy, «EIVA».

Митько А.В., Синицына А.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ГИДРОГРАФИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СУДОХОДСТВА. ГИДРОМЕТЕОРОЛОГИЧЕСКАЯ ПОДДЕРЖКА ИНЖЕНЕРНЫХ ИЗЫСКАНИЙ

На сегодняшний день гидрографическое обеспечение судоходства является обширной областью, занимающейся изучением морского дна. Однако, помимо океанографических и промысловых задач, перед гидрографией, в первую очередь, стоит задача изучения и выявления навигационных опасностей, а также поддержка строительства гидротехнических сооружений. Без должного изучения строения морского дна и тенденций его изменения представляется невозможным производить строительство сложных инженерных строений и объектов, связанных с морским пространством.

Однако, любые инженерные изыскания требуют должной гидрометеорологической поддержки. Из опыта проводимых мной гидрографических работ я могу с уверенностью сказать, что даже на мелководных акваториях заливов при постоянных ветрах образуются значительной силы волны,

которые представляют опасность не столь для качественного выполнения работ, сколько для экипажей маломерных гидрографических катеров.

Поэтому, безопасность навигации зависит не только от гидрографических изысканий, но и во многом от предоставления качественных гидрометеорологических прогнозов. Знание и умение правильно оценивать природные процессы позволяют морякам избегать опасных явлений, бороться за жизнеспособность судна.

Таким образом, можно подвести небольшой итог: морская деятельность не является чем-то обособленным, это сложный и многомерный комплекс изучения Мирового океана, ресурсопотребления и сохранения экологической обстановки, поэтому так важно обеспечить безопасность выполнения различного рода работ. Такими гарантами во многом являются гидрография и гидрометеорология. Развитие этих двух отраслей хотя и идет каждый своим путем, но неразрывно связано и призвано служить одному делу.

Митько А.В., Сальцберг Э.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

АНАЛИЗ ПРАВОВЫХ АСПЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Рассматривая современное состояние и значение морских перевозок, рост их роли и объема грузооборота, увеличение численности торговых, рыболовецких и военно-морских судов, и как следствие - усиление конкуренции в данных сферах деятельности, необходимо отметить их возрастающую зависимость от информационных технологий и современных морских навигационных систем, а, следовательно, уязвимость информационной безопасности объектов морской техники и морской инфраструктуры.

В связи с чем, надёжная зашита морских коммуникаций, в число которых входят и морские транспортные средства и их оборудование, является одним из важных условий достижения успеха.

В настоящее время, когда безопасность стала зависеть от всех составляющих ее элементов, когда нарушение в доступе одного из них, ведет к негативным последствиям для всей системы, огромную роль в развитии информационной безопасности играют не только программы и специальные информационные системы, непосредственно направленные на обеспечение необходимой конфиденциальности (защищенности от уничтожения, изменения, блокирования, а также иных несанкционированных действий), но и усиление правовой базы, регламентирующей законность их создания и применения (как пример можно привести юридическую ответственность за создание программных вирусов, взлом сетей госструктур и коммерческих организаций и т.п.).

Исходя из изложенного, целью работы стал анализ существующей нормативно-правовой базы, регламентирующей обеспечения информационной безопасности объектов морской техники и морской инфраструктуры.

В заключение: Проведенный анализ правовых аспектов информационной безопасности объектов морской техники и морской инфраструктуры (в зависимости о выбранной темы, позволил сделать выводы об отставании законодательных норм от существующих потребностей и реалий морской инфраструктруры и позволил сделать выводы о необходимости.

Минина М.В.., Сальцберг Э.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Вместе с тем, информация это весьма специфический продукт, который может быть как в материальном, так и в нематериальном (нефиксированном) виде. Поэтому, без четких границ, определяющих информацию, как объект права, применение любых законодательных норм по отношению к ней - весьма проблематично.

Основные гарантии информационных прав содержатся в Конституции РФ. Несмотря на то, что Конституция является законом прямого действия, применить ее положения к отдельным видам отношений без последующей конкретизации было бы затруднительно. Отдельные виды отношений регулируются специальными законами, которые, как правило, так же не содержат норм, непосредственно устанавливающих правила информационного взаимодействия.

Правила информационного взаимодействия, возникающего в ходе осуществления конкретных отношений, регулируются на уровне постановлений Правительства, либо ведомственных нормативных актов. При этом, на данном уровне, как правило, создается нормативный акт, обязательный для участников этих отношений, а его устанавливаемые в нем правила доводятся до сотрудников или структурных подразделений соответствующего государственного органа путем издания инструкции или рассылки письма.

Для оптимизации информационной безопасности можно прибегнуть к 3 мерам противодействия, так называемого хакерского нападения: правовому, организационно-административному и инженерно-техническому. Все вышеуказанные типы защиты информации и их элементы тесно взаимосвязаны друг с другом, пересекаются и объединяются, интегрируясь, в единую систему. Только сочетание различных форм и содержащихся в них задач может обеспечить надежность защиты данных. Каждый из этих элементов, составляющих соответствующие подсистемы защиты информации, важен и неотъемлем от всей системы. Однако на современном этапе развития средств и ресурсов информатизации на центральное место в ней выходят правовая и программная системы защиты информации, оставляя за административной и физической системами роль организационного и технического обеспечения защиты. Тип защиты данных определяется объектом защиты и характером взаимодействия с ним:

- содержанием и формой защиты;
- подходом к защите, обязательным или добровольным;
- целью и назначением защиты;
- уровнем защиты информации.

Содержание и форма защиты определяют ее вид - правовой, организационно-административной и инженерно-технической.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ

Алексеева-Попова Н.В., Дроздова И.В., Калимова И.Б., Беляева А.И.
Россия, Санкт-Петербург, Ботанический институт им. В.Л. Комарова Российской академии наук

ПЕРСПЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АККУМУЛИРУЮЩИХ СВОЙСТВ РАСТЕНИЙ ДЛЯ СНИЖЕНИЯ РИСКА ЗАГРЯЗНЕНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ ТЯЖЕЛЫМИ МЕТАЛЛАМИ

Среди загрязнителей среды все больший удельный вес приобретают тяжелые металлы, повышенные концентрации которых представляют опасность для биоты, в том числе для человека. Наряду с многочисленными способами снижения уровня токсикантов в среде: техническими, механическими, химическими в последнее время привлекают внимание биологические методы. Они обладают рядом преимуществ: не требуют дорогостоящего оборудования, дешевле обычных методов ремедиации, экологически безопасны. Среди методов фиторемедиации наибольший интерес представляет фитоэкстракция токсикантов с использованием растений - гипераккумуляторов (ГА) тяжелых металлов.

К гипераккумуляторам относятся виды растений, накапливающие в своих тканях > 1000 мг/кг Ni, Cu, Cd, Pb, Co или > 10 000 мг/кг Zn, Mn. Количество видов ГА ограничено, они встречаются только в 34 из 400 семейств цветковых растений, большинство видов ГА относится к сем. Cruciferae (крестоцветные). В настоящее время известно 360 видов-гипераккумуляторов Ni, 34 вида – Cu, 30 видов - Co, 15 видов - Zn, 14 видов - Pb и 3 вида - Cd. Растения - гипераккумуляторы обитают преимущественно в южных широтах, часто в районах обогащения тяжелыми металлами, многие из них являются эндемичными видами. Ремедиация почв с использованием ГА тяжелых металлов применяется в ряде стран, но не является широкомасштабной из-за незначительного количества видов ГА и некоторых их свойств.

Основным препятствием в эффективном использовании этих видов является трудность культивирования эндемичных видов, низкая скорость их роста и накопления биомассы. Поэтому перспективными для целей фиторемедиации могут быть широко распространенные виды синантропных флор, однако их аккумулирующая способность не исследована.

Мы изучали накопление тяжелых металлов у 15 видов крестоцветных, произрастающих на территории Ботанического сада БИН РАН и в городских посадках Санкт-Петербурга. Было определено содержание Cu, Ni, Zn, Cd, Pb в надземных органах, а также корнях растений и уровень подвижных форм этих элементов в почвах. Найдены межвидовые различия в накоплении тяжелых металлов, наибольшие – для Zn и Pb. Максимальным содержанием всех определявшихся элементов отличается вид Arabidopsis thaliana. Концентрация Pb в листьях этого вида составляет 50 мг/кг, а у другого вида - Thlaspi arvense из того же местообитания - лишь 4.5 мг/кг. Способностью повышенного накопления Cu не только в листьях, но и в корнях при значительной биомассе характеризуется широко распространенный рудеральный вид Capsella bursa-pastoris. Вид Brassica juncea отличается максимальной интенсивностью накопления Ni в корнях, известно, что этот вид используется для очистки территорий, загрязненных Pb. Определение коэффициентов биологического накопления (отношение содержания элемента в растениях к содержанию в почве) отдельных элементов подтвердило максимальные величины интенсивности накопления ТМ для Arabidopsis thaliana. Однако, ни у одного из этих 15 видов в природных условиях не было выявлено гипераккумулирующей способности.

В экспериментальных условиях исследование потенциальных возможностей накопления тяжелых металлов было проведено на 7 видах крестоцветных, выращенных из семян, собранных на Северном Кавказе в районе обогащения почв тяжелыми металлами. Были поставлены модельные опыты в контролируемых условиях с внесением в питательную среду возрастающих доз тяжелых металлов: Zn, Cd, Ni в диапазоне: 5x10-5 М - 2x10-3 М. При повышенных дозах Zn в питательной среде в листьях растений накапливаются значительные количества Zn, намного превышающие таковые в природных условиях: у Neslia paniculata - до 1300 мг/кг, у Erysimum aureum - до 1600 мг/кг, у Alyssum gehamense - до 1650 мг/кг Zn. Очень высоким уровнем накопления Ni в надземных органах отличаются Alyssum tortuosum и Alyssum trichostachium: 3800 мг/кг и 2360 мг/кг соответственно. Следует отметить, что концентрация Ni в природных условиях у этих видов не превышает 8 мг/кг.

При внесении Cd в питательную среду его концентрация в листьях изученных видов резко возрастает, у Erysimum aureum – до 425 мг/кг. Для сравнения укажем, что даже на отвалах предприятий по добыче полиметаллических руд концентрации Cd в листьях крестоцветных не

превышает 1 мг/кг. Это свидетельствует о потенциальных возможностях аккумуляции Cd и перспективности использования этого вида для целей фиторемедиации.

Таким образом, в экспериментальных условиях было установлено, что максимальным содержанием Zn выделяется вид Alyssum gehamense, Zn и Cd – Erysimum aureum. У вида Neslia paniculata высокая аккумулирующая способность по отношению к Zn сочетается с относительно большой скоростью накопления биомассы. Виды рода Alyssum накапливают концентрации Ni, сопоставимые с уровнем элемента у видов-гипераккумуляторов. Изученные нами в экспериментальных условиях виды перспективны для использования в целях фиторемедиации техногенно загрязненных тяжелыми металлами территорий.

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

ФОРМИРОВАНИЕ И ИССЛЕДОВАНИЕ ВЫСОКОЭФФЕКТИВНЫХ ФОТОЭЛЕКТРИЧЕСКИХПРЕОБРАЗОВАТЕЛЕЙ НА ОСНОВЕ ГЕТЕРОСТРУКТУР АМОРФНЫЙ/МОНОКРИСТАЛЛИЧЕСКИЙКРЕМНИЙ

Актуальной задачей XXI века является решение долгосрочных энергетических проблем, связанных с исчерпаемостью традиционных источников энергии и ухудшением экологического состояния Земли В связи с обострением экологической ситуации в мире, а так же с уменьшением запасов углеводородов большое внимание в настоящее время уделяется поиску альтернативных, экологически чистых источников энергии. В частности, наиболее актуальным и перспективным направлением альтернативной энергетики на данный момент времени является солнечная фотоэнергетика.

Анализ тенденций развития рынка солнечной энергетики показывает, что при сохранении стоимости на кристаллический кремний на современном уровне в ближайшем будущем конкурентно способными будут технологии, обеспечивающие эффективность преобразования солнечного света порядка 20% и выше. Одной из наиболее привлекательных технологий изготовления солнечных элементов (СЭ) на основе кристаллического кремния (c-Si) является HIT (Heterojunction with Intrinsic Thin layer) технология, базирующаяся на формировании гетероперехода при помощи тонких пленок аморфного кремния (a-Si:H), нанесенных на поверхность пластины c-Si. СЭ изготовленные по такой технологии обладают всеми преимуществами классических СЭ на основе кристаллического кремния, включая высокую эффективность достигающую на сегодняшний день 24 % в промышленном производстве, что соответствует уровню рекордных величин для монокристаллического кремния. Дополнительными преимуществами этой технологии являются низкий, по сравнению с классическими СЭ на c-Si, температурный коэффициент снижения мощности и низкотемпературный процесс формирования таких структур, что позволяет использовать более тонкие пластины c-Si, и следовательно, производить более экономный расход материала, что невозможно при использовании высоких температур вследствие деформации пластин c-Si.

Использование гетероструктур является одним из наиболее эффективных способов подавления поверхностной рекомбинации. В солнечных элементах на основе гетероструктур могут применяться как анизотипные, так и изотипные гетеропереходы. Солнечное излучение падает со стороны широкозонного полупроводника, играющего, как правило, одновременно роль эмиттера – тонкого сильно легированного слоя. Основная часть излучения поглощается в узкозонном полупроводнике - базе, которая слабее легирована по сравнению с эмиттером и имеет большую толщину.

Основным отличием солнечных элементов (СЭ), изготовленных по технологии HIT, от классических СЭ на кристаллическом кремнии (c-Si) является наличие собственного слоя аморфного кремния (a-Si:H). Назначение этого слоя: формирование гетероперехода и пассивация дефектов на поверхности c-Si пластин. Пассивация дефектов необходима для снижения рекомбинации неравновесных носителей через поверхностные состояния. Недостаточная пассивация поверхности c-Si пластин приводит к снижению напряжения холостого хода, что влечет за собой снижение эффективности СЭ. Таким образом, качество пассивации поверхности c-Si пластин является одним из наиболее критических параметров для создания высокоэффективных СЭ на основе HIT структуры. Оценку качества пассивации производят путем измерения время жизни неравновесных носителей заряда, величина которого для создания высокоэффектиных HIT СЭ должно быть более 1 мсек после пассивации.Методы оценки качества пассивации в основном основаны на измерении времени релаксации проводимости после облучения импульсом света. В нашем случае для измерения времени жизни неравновесных носителей заряда использовалась стандартизированная измерительная установка SintonWCT-120 lifetimetester.

Исследования влияния условий обработки поверхности кремниевой подложки позволили выявить различия в технологическом подходе к формированию СЭ на Si подложках *p*- и *n*-типа проводимости. Показано, что обработка в H_2 плазме поверхности Sip-типа проводимости

(легированного бором) ухудшает характеристики (n)a-Si:H/(p)c-Si СЭ за счет пассивации легирующей примеси бора при диффузии водорода в приповерхностную область Si. Однако, исследования влияния слоя (i)a-Si:H на свойства границ раздела показали, что введение нелегированного слоя a-Si:H между легированными бором слоями a-Si:H и подложкой Si *n*-типа действительно позволяет повысить эффективное время жизни неосновных носителей заряда в Si, приводя к повышению КПД вплоть до 20 %. Следует отметить, что полученные результаты не являются рекордными. Так компания Sanyo, которая теперь принадлежит корпорации Panasonic, обладает рекордом эффективности таких солнечных элементов на сегодняшний день (25.6 %). Поэтому исследования гетероструктурных солнечных элементов на основе кремния целесообразно продолжать.

Биненко В.И.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук

ИНФОРМАЦИОННАЯ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРИ СОВРЕМЕННОМ ИЗМЕНЕНИИ КЛИМАТА

Нельзя со 100% вероятностью утверждать, что причиной наблюдаемого потепления климата отдельных регионов и Земли в целом напрямую связано с ростом концентрации парниковых газов ПГ. Но алармисты – климатологи, основываясь на докладах Международной Группы Экспертов по Изменению Климата (МГЭИК-IPCC), убеждены в антропогенном воздействии человека на климат и природу и в необходимости принятия незамедлительных мер для оптимизации системы природа общество. Мнения скептиков по данной проблеме связаны с существующими неопределённостями, обусловленными крайне неравномерным покрытием метеоданными земного шара, не учетом ряда климатических обратных связей, цикличностью климата, наличиемопределённой политизированности проблемы взаимосвязи климата и ПГ. Тем не менеесуществует необходимость сокращения выбросов ПГ, так как современное изменение климата сопровождается аномальными явлениями погоды последних лет, например, в РФ – наводнения на Амуре в 2013г,в Сочи в 2015г.,засухи,лесные пожары в Европейской части России в 2010 г., в Хакассии и Прибайкалье в 2015 и др. Поэтому важна реализация Экологической доктрины РФ о развитие государственной системы мониторинга окружающей среды в том числе климата и ПГ в России, так как она позволяет оценить насколько успешно будет проводиться модернизация промышленности и перестройка технологий производства энергии, направленной на резкое снижение энергоемкости отечественной продукции промышленности, сельского и лесного хозяйства.

В 2015 году, в части развития Киотского протокола подписанного в 1997г., планируется проведение конференции Сторон Рамочной Конвенции ООН по изменению климата, где планируется подписание нового глобального соглашения по изменению климата и сокращению выбросов ПГ, по развитию возобновляемых источников энергии субсидий на ископаемое топливо, по сохранению лесов на планете.

В докладе будут рассмотрены особенности климатической политики в России в рамках глобальной стратегии до 2050 г. Сокращение выбросов CO_2 (%) в РФ за период с 1990 по 2012 гг. был 27.9% **,**ак 2050 году, планируется сокращение выбросов – минус 80% от уровня 1990 года.

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

КОМПЛЕКСНЫЙ МОНИТОРИНГ СОСТОЯНИЯ ПРИПРОДНОЙ СРЕДЫ – ОСНОВНОЙ ИСТОЧНИК ИНФОРМАЦИИ ОБ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА

Информационная безопасность – одна из важнейших задач при определении экологического состояния региона и прогнозирования возможных его изменений.

Это связано с тем, что поступающая в центры экологическая информация может подвергаться искажениям различного характера, устранение которых требует сведений о достоверности и точности проведенных измерений. В настоящее время разработано большое количество различных контактных и дистанционных датчиков для измерения отдельных параметров состояния природной среды, работающих на разных физических принципах в различных диапазонах электромагнитного излучения. Проверка их совместимости может проводиться при выполнении комплексных экспериментах на эталонных участках. Впервые такая работа по комплексным измерениям параметров природной среды наземными, воздушными и космическими датчиками была проведена при выполнении комплексных подспутниковых экспериментов по инициативе академика К.Я.Кондратьева под руководством Бузникова А.А еще в 1969-70 гг. над пустыней Кара-Богаз гол между Каспийским и Аральским морями. Они дали большой объем информации о состоянии природных объектов и позволили оптимизировать данные о конкретных параметрах состояния природной среды. В настоящее время эта методика стала основной при дистанционном зондировании природной среды с аэрокосмических носителей. В докладе рассматривается

необходимость валидации спутниковых данных по результатам наземных измерений и необходимость проведения комплексных экспериментов при проведении мониторинга природной среды отдельных регионов с целью обеспечения их экологической безопасности.

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

ИССЛЕДОВАНИЕ УЛЬТРАФИОЛЕТОВЫХ ФОТОПРИЕМНИКОВ НА ОСНОВЕ КАРБИДА КРЕМНИЯ

Разработка датчиков ультрафиолетового излучения связана с сохраняющимся интересом использования их в медицине, армии и других областях науки и техники, а так же экологии при изучении проблемы «озоновых дыр». Но для того чтобы регистрировать только УФ излучение нужно использовать широкозонные полупроводники. В качестве исходного материала было предложено использовать карбид кремния политипной модификации 4H, который имеет ряд преимуществ по сравнению с широкозонными материалами группы $A^{III}B^{V}$, таких как малая плотность дефектов, слабая деградация при мощном УФ излучении, высокие рабочие температуры и теплопроводность.

Для исследований были получены $p^+–p–n^+$ и $p^+–n–n^+$ 4H-SiC фотоприемники УФ –излучения. В качестве подложки использовался n^+ 4H-SiC размером 1400×1400 мкм. Размер активной области после травления составлял 700×700 мкм. Травление мезо структуры осуществлялось для уменьшения поверхностных токов утечки. Глубина мезы определялась глубиной p-n перехода и составляла 2-3 мкм для $p^+–n–n^+$ и 9 мкм $p^+–n–n^+$. Угол составлял примерно 70°-80°. На подложке был выращен согласующий n^+ 4H-SiC слой, легируемый азотом, с концентрацией примеси $5·10^{18}$ $см^{-3}$ и толщиной 1 мкм. Для i слоя были использованы слои n и p типа проводимости, легируемых азотом и алюминием соответственно, с концентрацией примеси $6·10^{14}$ $см^{-3}$ и толщиной 6 мкм. Легированный алюминием верхний p^+ 4H-SiC слой имел толщину 0,4 мкм и концентрацию примеси около 10^{19} $см^3$.Омический контакт к подложке состоял из Ti/Ni, а к p^+ слою из Al/Ti/Ni толщиной 2мкм.

В зависимости от типа проводимости базового слоя область пространственного заряда находилась на разной глубине от поверхности, на которую падало ультрафиолетовое излучение, что влияло на смещение максимума спектральной чувствительности. В связи с этим при подаче обратного напряжения можно добиться высокой селективности УФ фотоприемников.

Измерения фототока проводились при помощи пикоамперметра Keithley 6482, он же являлся и источником обратного напряжения. В качестве источника излучения служила ксеноновая лампа совместно с монохроматором М266, с помощью которого выделялись узкие спектральные интервалы. Образец располагался у выходной щели монохроматора. В качестве эталона использовался откалиброванный кремниевый фотоприемник ФДУК -100 УТ. Обратное напряжение подавалось в диапазоне от 0 до -10В, дальнейшее увеличение напряжения влияло на смешение максимума незначительно.

В процессе измерения были получены спектральные зависимости с краем поглощения 390 нм. При увеличении обратного напряжения максимум спектральной чувствительности смещался в коротковолновую область спектра и увеличивал свое максимальное значение. Это связано с расширением области пространственного заряда и смещением ее в приповерхностную область. Вследствие чего большее количество высокоэнергетических квантов участвуют в процессе генерации, так как все излучение поглощается в тонком приповерхностном слое.

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

ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАТИВНЫХ ПАРАМЕТРОВ О ДЕЙСТВИИ ИНГИБИТОРОВ ДЫХАТЕЛЬНОГО ПУТИ НА ТЕРМОТАКСИЧЕСКУЮ РЕАКЦИЮ ПРОСТЕЙШИХ

Информационная безопасность предполагает необходимость технических разработок, направленных на обеспечение защищенного состояния объекта, которым в наше время выступает не только антропогенные объекты, но и окружающая среда. Важнейшим видом информации для защиты среды являются информативные параметры для детектирования новых угроз, локальных и глобальных на основе данных, получаемых методами не только физико-химического, но и биологического контроля.

Температурные изменения среды, проявившиеся в последнее десятилетие, обусловливают необходимость контроля реакций организмов на эти изменения.

Перспективной тест-реакцией для контроля воздействия температур на популяцию одноклеточных является термотаксис организмов, который представляет собой их перемещение в зону комфортных температур и изучается с конца XIX века (метод Гертера). Но лишь в начале XXI века было выявлено, что свойства термотаксиса инфузорий имеют сходство с температурной

регуляцией многоклеточных. Одноклеточные организмы, не обладая нервной системой, образуют плавающие структуры, способные находить зону температурного оптимума.

На данный момент является актуальной задачей исследование возможности практического использования открытого в 2000-х гг. свойства инфузорий – отражения в реакции термотаксиса воздействия ингибиторов фосфорилирования и построения на основе экспресс-биотеста.

Ранее разработан экспресс-метод проверки термочувствительности инфузорий для создания биотестовой системы контроля загрязнений водных сред. С помощью нового метода исследована термочувствительность инфузорий Paramecium caudatum разного возраста. Но оставалась сложность с автоматизацией процесса обработки данных.

Создание системы контроля тест-реакции термотаксиса, которая включает в себя аппаратурную часть (систему на базе цифровой камеры с режимом макросъемки) и программную часть (программу цифровой и статистической обработки изображений простейших), позволит усовершенствовать и упростить процесс обработки результатов экспериментов.

Программная часть системы контроля термочувствительности простейших позволяет произвести расчет информативных параметров реакции термотаксиса инфузорий с помощью источника холода, находящегося с одной стороны узкой протяженной кюветы.

Раскодировка видеофайлов в разработанной программе происходит автоматически по заданным оператором параметрам. Скорость обработки составляет 12 видеозаписей/мин. В качестве информативных параметров тест-реакции был выбран угол наклона линейного тренда популяционного распределения простейших относительно времени воздействия источника холода.

Созданная система контроля таксических реакций дала возможность провести апробацию нового биотестового подхода, позволив перейти к экспериментам с токсикантами: сульфатом меди, воздействующий на метаболизм, в т.ч. дыхание, и азид натрия, влияющий только на дыхание.

Полученные результаты: обоснована актуальность экспресс-метода контроля загрязнений водных сред на базе тест-реакции термотаксиса; разработана программа обработки цифровых видеоизображений, которая обладает модулем, обеспечивающим целостность и доступность информации; предложен информативный параметр для тест-реакции – распределение угла наклона линейного тренда распределения клеток по узкой протяженной кювете во времени.

Венедиктов В.Ю., Горелая А.В., Шалымов Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ГРОЗОВЫХ ОБЛАКОВ С ПОМОЩЬЮ ЭФФЕКТА КЕРРА

Исследования величины напряженности, а также пространственно-временной структуры электрических полей над грозовыми облаками, до исразу же послеразряда молнии, необходимыдля пониманияэлектродинамических эффектовтропосферы и всей атмосферы в целом. В настоящее времятакие поля могутбытьизмерены только локально, либо около поверхности планеты, либо в отдельных областях вблизи или внутриоблака (с помощью зондов или беспилотных самолётов). Такие измеренияне позволяютточно оценитьобщую структуру полейвнутри и за пределамиоблака. Кроме того, запуск, эксплуатация и восстановление зондов (из-за жестких условий эксплуатации) и, устанавливаемых на их борту, экспериментальных установок приводит к повышенным материально-техническим затратам. Использованиеметодов дистанционного зондированияможет решитьпроблемы, описанные выше.

Относительно недавно был разработан метод дистанционного зондированияэлектрических полей грозовых облаков посредством явления электрически индуцированного двойного лучепреломления (эффекта Керра), изменяющего природную поляризацию света, рассеянного атмосферой.

В результате двулучепреломления возникает различие в показателях преломления волн, поляризованных параллельно и перпендикулярно приложенному полю. Это приводит к фазовому сдвигу, измеряя который можно определить амплитуду электрического поля.

Кроме эффекта Керрав атмосферевстречаются и другиеявления, которые могутвызватьдвойное лучепреломление. Сильныепотоки воздухатакжемогут изменить природную поляризацию света, рассеянного атмосферой [G. R. Boyer, B. Lamouroux, B. S. Prade, 1977].

Были рассчитаныфазовые сдвиги, вызываемые: эффектом Керра при типичной грозе $\varphi k \approx 10\text{-}5$(рад) иатмосферным течением $\varphi f \approx 2\times 10\text{-}6$(рад). Так как значения сдвигов фаз сравнимы, то влиянием воздушных потоков на состояние поляризации света рассеянного атмосферой пренебрегать нельзя. Измерять напряжённость электрического поля с помощью метода предложенного в статье [S B. E. Carlson, U. S. Inan, 2008] нельзя. Однако, модифицировав этот метод можно исключить влияние градиента скорости ветра.

Викторов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук,
Санкт-Петербургский государственный университет

СОВРЕМЕННАЯ МОРЕХОЗЯЙСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ В ФИНСКОМ ЗАЛИВЕ СКВОЗЬ ПРИЗМУ ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Обсуждается развитие морехозяйственной деятельности в восточной части Финского залива Балтийского моря. Основное внимание уделено морскому транспорту. Отмечен небывалый рост морских перевозок опасных грузов за последние 15 лет. Анализируются различные факторы воздействия морского транспорта на окружающую морскую и береговую среду. Обсуждаются текущие проблемы использования методов дистанционного зондирования в комплексном экологическом мониторинге состояния акватории и атмосферы.

Горохов В.Л., Бузников А.А., Федкович О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КОГНИТИВНЫЙ МОНИТОРИНГ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ НА ОСНОВЕ МНОГОМЕРНЫХ ДАННЫХ РЕГИОНАЛЬНЫХ СЛУЖБ ЗДРАВООХРАНЕНИЯ

Современные реформы системы российского здравоохранения предполагают осуществление оптимизации работы медицинских учреждений в регионах. Поскольку сами учреждения достаточно многочисленны (более 1300 объектов) и характеризуются значительным набором контролируемых параметров (более тридцати параметров), задача интегральной оценки их состояния представляет собой достаточно сложную задачу многофакторного анализа. Поскольку на функционирование медицинских учреждений влияет и достаточно нестационарный поток поступления пациентов задача анализа еще более усложняется. Поэтому предварительный анализ ситуации наиболее успешно может выполняться при наличии компьютерных средств когнитивной визуализации многомерных данных мониторинга учреждений здравоохранения.

В данной работе демонстрируются возможности классификации состояния медицинских учреждений средствами когнитивной визуализации (программная система SW-20) многомерных данных их мониторинга.Использовались стандартный набор параметров по которых характеризуются современные медицинские учреждения. В типовой перечень были включены следующие параметры: отчетный период – дата окончания лечения.

Рассматривались следующие случаи лечения:

– дневной стационар;
– досуточная госпитализация;
– госпитализация более суток.

Comid_case – идентификатор случая в информационных системах ID_JUR – идентификатор MODEPART – идентификатор отделения МО, DATE_IN – дата начала случая лечения, DATE_OUT – дата окончания случая лечения, AMOUNT_REAN – дней в реанимации, DIAGN – диагноз основной, SEX – пол, BIRTHDAY – дата рождения, ORDER –порядок направления,ID_LPU_ATT – идентификатор МО прикрепления застрахованного, sum_case – сумма всего случая, sum_gosp – сумма случай образующего КСГ без приложений № 5, 5-1 и 5-2, sum_5 – сумма случай образующего КСГ только приложения №5, 5-1 и 5-2, sum_rean – сумма реанимаций, sum_anest – сумма анестезий, sum_oper – сумма операций, sum_dop – сумма тарифов ДопТ, ДопВ, sum_other – сумма прочего, NOM_KODES – номенклатурные коды операций, DOP_NOM_KODES – дополнительные номенклатурные коды операций, PRIZ_HMP_B – признак базовой ВМП , PRIZ_HMP_SB – признак сверхбазовой ВМП, PRIZ_REABILIT – признак реабилитаций , PRIZ_DSTAC – признак дневного стационара. Удалось ввиде одного когнитивного образа представить 1416 медицинских учреждений Северо-западного региона.

Этот образ был представлен в виде псевдо-трехмерного облака точек, где каждая точка описывалась выше перечисленными параметрами, которые выступали координатами в многомерном пространстве данных. Особенности структуры этого псевдо трехмерного образа обеспечили выявление и классификацию состояния этих учреждений.

На основе такой классификации удалось выявить, как наиболее успешные, так и недостаточно правильно функционирующие учреждения. Многомерный статистический анализ, проведенный с учетом интерпретации когнитивного образа обеспечивает объективацию полученных решений.

Следует особо подчеркнуть что эффект выявления опасных тенденций в работе объектов когнитивного мониторинга плохо выявляется с помощью более традиционных средств обнаружения и контроля.

Горяинов В.С., Бузников А.А., Черноок В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), ОАО «Гипрорыбфлот»

АВТОМАТИЗАЦИЯ ОЦЕНКИ ВЕРОЯТНОЙ ИНФОРМАТИВНОСТИ ЛИДАРНОГО ЭХО-СИГНАЛА

Оптические локаторы (лидары) представляют мощный инструмент экологического мониторинга и обеспечения экологической безопасности. Выбор необходимой длины волны зондирующего излучения и информативных параметров эхо-сигнала позволяет, в зависимости от решаемой задачи, определять присутствие и характер взвеси в водной среде, измерять прозрачность, концентрацию фитопланктона и растворённого органического вещества, обнаруживать загрязнения, в том числе нефтяные.

В то же время высокое пространственное и временное разрешение лидарных систем приводит к необходимости обработки значительных объёмов данных. Изменения внутренних параметров системы и внешних условий могут выводить лидарную систему из рабочих режимов. Очевидно, эхо-сигналы, зафиксированные за пределами рабочих режимов, содержат искажённое представление о среде и объектах зондирования или вовсе не несут полезной информации. Визуальная оценка человеком информативности конкретного сигнала по его форме трудоёмка и занимает много времени.

В представленном докладе описывается ряд подходов к автоматизации оценки информативности лидарного эхо-сигнала. Задачей каждого из методов является разделение набора эхо-сигналов по их вероятной информативности.

По степени участия человека в процессе «сортировки» эхо-сигналов описанные методы располагаются в следующем порядке.

Сортировка по характерным признакам. В имеющемся наборе сигналов выделяется ряд критериев формы, по соответствию которым эхо-сигналы делятся на несколько групп (шум, искажённый сигнал, неискажённый сигнал).

Применение искусственных нейронных сетей. В наборе сигналов выбираются несколько групп эхо-сигналов с характерной формой. Искусственная нейронная сеть обучается на сигналах из этих групп, а затем разделяет остальные сигналы по степени их сходства с образцами.

Применение самоорганизующихся сетей и карт. Метод является развитием предыдущего. Самоорганизующаяся нейронная сеть не требует для своего обучения образцов. Получив на входе полный набор эхо-сигналов, сеть самостоятельно выделяет в них ряд характерных признаков и делит предоставленные ей сигналы на группы по их вероятной информативности.

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

ПРИМЕНЕНИЕ СИСТЕМЫ ПРОСТРАНСТВЕННОГО ПОЗИЦИОНИРОВАНИЯ СОЛНЕЧНЫХ МОДУЛЕЙ С ЦЕЛЬЮ ПОВЫШЕНИЯ ИХ ЭФФЕКТИВНОСТИ В УСЛОВИЯХ ИЗМЕНЕНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ

Фотоэлектрическое преобразование солнечной энергии является одним из наиболее быстро развивающимся в мире направлением использования возобновляемых источников энергии. Преимущества технологий, использующих энергию солнца, в том, что при работе солнечных установок практически не добавляется тепло в приземные слои атмосферы, не создается тепличный эффект и не происходит загрязнения воздуха. Но у солнечной энергии есть недостаток - ее зависимость от состояния атмосферы, времени суток и года.

В работе предлагается установление слабоконцентраторных систем, предназначенных для повышения освещенности модулей. Главным требованием к их выходным энергетическим характеристикам является обеспечение равномерного распределения лучистого потока на приемной поверхности. Исходя из этого условия были реализованы концентраторы с плоскими отражающими поверхностями на основе односекционных и многосекционных вариантов плоских систем. Односекционные плоские системы позволяют получать 2-10 кратную концентрацию солнечного излучения при приемлемых массогабаритных показателях и обеспечивать достаточно равномерное распределение плотности лучистого потока на приемнике при неточной ориентации концентратора на солнце и деформации его отражающих поверхностей. Учитывая температурные характеристики готовых модулей, полноценную работоспособность солнечная панель показывает при 3-х кратном коэффициенте концентрации. Для подобного увеличения плотности потока можно не устанавливать теплоотвод, а угол раскрытия отражателей лежит в пределах 60˚.

Для более чем 3-х кратной концентрации предлагается применять многосекционные плоские системы, в основном из-за существенного уменьшения габаритов. Угол раскрытия каждой секции выбирается таким образом, чтобы отраженные лучи попадали на поверхность приемника после однократного отражения. При 3-х кратной концентрации достаточно 2-х секционных отражателей по бокам с углом наклона первой секции 60˚. Расчеты показали, что такое соотношение получается

оптимальным и позволяет достичь минимальной глубины фоклина. При любых других значениях концентрации необходим теплоотвод и пересчет углов.

В данном случае речь идет о слабоконцентраторных системах, предназначенных для повышения освещенности модулей. Поэтому важным требованием к их выходным энергетическим характеристикам является обеспечение равномерного распределения лучистого потока на приемной поверхности. Исходя из этой точки зрения были выбраны концентраторы с плоскими отражающими поверхностями. Были реализованы односекционные и многосекционные варианты плоских систем.

Таким образом, дляповышения эффективности работы солнечных модулей в данной работе была реализована система концентрации оптического излучения, позволяющая принимать излучение в широком угловом поле и с возможностью увеличения оптического КПД на 50% с кратностью концентрирования от 3 до 10х вне зависимости от состояния окружающей среды.

Доронин А.П., Щукин Г.Г., Дидык О.И., Козлова Н.А., Петроченко В.М., Фролов К.О., Шмалько С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПЕРЕЧЕНЬ ЭКОЛОГИЧЕССКИХ ПРОБЛЕМ, РЕШЕНИЕ КОТОРЫХ ВОЗМОЖНОПРИ МОДИФИЦИРОВАНИИ ОБЛАКОВ И ТУМАНОВ ЕСТЕСТВЕННОГО И ИСКУССТВЕННОГО ПРОИСХОДЕННИЯ

Наличие в современных условиях серьезных экологических проблемв нашей стране (загрязнение атмосферного воздуха в крупных промышленных районах, лесные пожары, смоги в мегаполисах и др.) обуславливает необходимость разработки и практического внедрения методов и средств борьбыс ними. В последние годы в качестве таковых предлагается применять методы и средства модифицирования геофизических процессови явлений (ГФПЯ). Исходя из этого, представляется важным проведение исследований по обоснованию перечня экологических проблем, решаемыхпри модифицировании ГФПЯ.

В частности, был проанализирован перечень таких проблем применительно к облакам и туманам естественного и искусственного происхождения. Установлено, что воздействия на облака и туманы естественного происхождения проводятся, как правило,с целью вызывания (интенсифицирования) осадков и рассеяния (стабилизации) облаков. При этом перечень прикладных задач, решаемыхпри каждом виде воздействия, может быть вполне определенным. При создании искусственных облакови туманов также может быть решен ряд вполне конкретных прикладных задач в интересах устранения возникающих экологических проблем.

Доронин А.П., Дидык О.И., Козлова Н.А., Петроченко В.М., Шмалько С.А., Фролов К.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПЕРЕЧЕНЬ ГЕОФИЗИЧЕСКИХ ПРОЦЕССОВ И ЯВЛЕНИЙ КАК ВОЗМОЖНЫХ ОБЪЕКТОВ МОДИФИЦИРОВАНИЯ В ИНТЕРЕСАХ РЕШЕНИЯ ЭКОЛОГИЧЕСКИХ ПРОБЛЕМ

Появившиеся в последние десятилетия возможности по модифицированию геофизических процессов и явлений (ГФПЯ) для решения широкого круга прикладных задач обусловливают необходимость обоснования перечня таких процессов и явлений как потенциальных объектов воздействия.

Результаты выполненного в этом направлении исследования приведены ниже.Установлено, что в:

– литосфере (1) основными процессами и явлениями как возможными объектами модифицирования могут быть: (1.1) сейсмические процессы; (1.2) вулканы; (1.3) склоновые процессы; (1.4) огненные бури; (1.5) ледники; (1.6) почвенный покров; (1.7) растительный покров;

– гидросфере (2) – процессы, наблюдающиеся в мировом океане (2.1), а именно: (2.1.1) процессы испарения с водной поверхности; (2.1.2) процессы волнения моря; (2.1.3) волны типа цунами; (2.1.4) ледовая обстановка; (2.1.5) тропические циклоны (ураганы и тайфуны) и гидрологическая обстановка суши (2.2), воздействие на которую целесообразно проводить с целью модифицирования наводнений, половодий, паводков (2.2.1) и с целью модифицирования состояния почво-грунтов (2.2.2);

– атмосфере (3) – конвективные облака и градовые процессы (3.1), включающие в себя следующие виды воздействия: (3.1.1) вызывание искусственных осадков; (3.1.2) интенсифицирование естественных осадков; (3.1.3) предотвращение выпадения осадков, (3.1.4) предотвращение выпадения града; (3.1.5) предотвращение возникновения гроз, - слоистообразные облака и туманы (3.2), включающие в себя следующие виды воздействия: (3.2.1) рассеяние переохлажденных облаков и туманов; (3.2.2) рассеяние теплых облаков и туманов; (3.2.3) вызывание искусственных осадков; (3.2.4) интенсифицирование естественных осадков; (3.2.5) стабилизация переохлажденных облаков и туманов; (3.2.6) стабилизация теплых облаков и туманов, - искусственные облака и туманы (3.3), включающие в себя воздействия с целью: (3.3.1) создания перистых кристаллических облаков; (3.3.2)

создания конвективных облаков; (3.3.3) создания слоистообразных облаков; (3.3.4) создание туманов; (3.3.5) создание низковысотных водно-аэрозольных образований;

– околоземном космическом пространстве (4), где основными объектами воздействия могут быть ионосфера (4.1), воздействие на которую может осуществляться с целью изменения концентрации электронов (4.1.1) и с целью инициирования полярных сияний (4.1.2), радиационные пояса Земли (4.2), а также магнитосфера (4.3).

На основе приведенных выше данных о возможных объектах модифицирования можно утверждать, что в интересах решения экологических проблем на современном этапе возможно и целесообразно осуществлять модифицирование следующих ГФПЯ: 1.3; 1.5; 2.1.5; 2.2.1; 3.1.1-3.1.5; 3.2.1-3.2.6; 3.3.1-3.3.5. Например, путем рассеяния облаков можно осуществлять очищения воздушных бассейнов крупных городов от вредных примесей (особенно в холодное полугодие). Путем вызывания искусственных и интесифицирования естественных осадков представляется возможным осуществлять тушение лесных пожаров и профилактику их возникновения.

Следует заметить, что по мере развития науки и техники возможности человека будут возрастать и, следовательно, будут также расширяться как перечень ГФПЯ, поддающихся воздействию (а в дальнейшем также и управлению), так и перечень экологических проблем, решаемых при воздействии на них.

Дроздова И.В., Шилин Б.В.
Россия, Санкт-Петербург, Ботанический институт им. В.Л. Комарова Российской академии наук, Центр экологической безопасности Российской академии наук

РАННЯЯ ДИАГНОСТИКА СТРЕССА РАСТИТЕЛЬНОСТИ И ЗАГРЯЗНЕНИЯ ПОЧВЫ ТЯЖЁЛЫМИ МЕТАЛЛАМИ ВИДЕОСПЕКТРАЛЬНЫМ МЕТОДОМ

Одна из проблем экологической безопасности – обнаружение загрязнения растительности и почв тяжёлыми металлами на ранних стадиях антропогенного воздействия. На основе полевых измерений спектральных характеристик растений новым методом дистанционного контроля – видеоспектральной съёмкой - выявлена быстрая отчетливая ответная реакция растительности на действие стрессовых факторов на ранних стадиях их воздействия в виде изменения значений коэффициентов спектральной яркости (КСЯ) в видимом и ближнем инфракрасном диапазонах 0.4 – 0.9 мкм. Экспериментальными данными показано, что видеоспектральная съёмка является эффективным методом регистрации стресса растительности на ранних стадиях антропогенного воздействия – загрязнения тяжёлыми металлами. Это, в свою очередь, является важнейшим ранним индикатором загрязнения тяжёлыми металлами почвенного покрова. Спектральная аномалия возникает через два-три дня после внесения в почву солей меди, никеля и кадмия и сохраняется длительное время.

Елизаров В.В., Кащеев С.В.,Гришканич А.С., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

НОВЫЕ ПОДХОДЫ К РАЗРАБОТКЕ АППАРАТНО-ПРОГРАММНОЙ СИСТЕМЫ УПРАВЛЕНИЯ И РЕГИСТРАЦИИ ЛИДАРНЫХ СИГНАЛОВ В ГИГАГЕРЦОВОМ ДИАПАЗОНЕ ЧАСТОТ

Лазерное зондирование может служить высокоэффективным методом дистанционного оперативного экологического мониторинга на суше и над поверхностью водных объектов. Искомыми веществами могут быть различные вещества-индикаторы утечек углеводородов из трубопроводов и перерабатывающих предприятий, токсичные агенты использующиеся для химических производств, дым от пожаров и т.д. Однако, для обеспечения высокой скорости зондирования, оперативности обработки получаемой информации и удобства управления лидарными установками необходимо использовать соответствующие программно-аппаратные комплексы, применяемые для решения задач сбора, обработки, накопления, систематизации больших массивов данных.

Создание таких комплексов задача не тривиальная, так как каждый из них должен отвечать ряду определенных требований зависящих от поставленной задачи. В разных типах лидарных установок используются разные типы лазерной спектроскопии

В рамках одного из проектов по разработке систем дистанционного зондирования, создана полнофункциональная аппаратно-программная система автоматизирующая процессы управления, сбора и обработки информации, получаемой в ходе зондирования с борта вертолёта МИ-8, что позволяет производить высокоскоростное, площадное исследование подстилающей поверхности. Основным преимуществом данной системы является возможность определения широкого спектра веществ загрязнителей, а так же возможность регистрации веществ с концентрацией на уровне фоновых значений в автоматизированном режиме (порядка 10-500ppb). Для реализации системы с такими возможностями, необходимо использовать ряд инженерных решений, таких как работа в гигагерцевом диапазоне частот с автоматизацией процесса сбора данных и ультараспектральное

разрешение. Ультраспектральное разрешение достигается особой реализацией оптического канала и приемной оптики. Для работы в гигагерцевом диапазоне частот использован набор специализированных как программных, так и аппаратных средств и особая модульная организация с возможностью синхронизации компонентов.

Каждая составная часть лидарной системы должна отвечать ряду требований, продиктованных работой в гигагерцовом диапазоне частот. Поэтому необходимо выбирать как аппаратные, так и программные решения, которые позволят реализовать высокоскоростной обмен данными между частями системы и высокоскоростную обработку получаемых данных и параметров системы.

С аппаратной точки зрения, проблема решается использованием модулей и составных частей с высоким быстродействием, а так же интерфейсов которые позволяют выполнять обмен данными с высокой частотой, что бы исключить потерю данных за счет временных задержек.

Программные модули используемые для управления, обработки и организации систем баз данных должны иметь соответствующие алгоритмы работы позволяющие в режиме реального времени выполнять обработку информации. В виду того, что в состав лидарной системы входят компоненты, которые должны взаимодействовать между собой, обмениваться данными и сигналами управления, каждый компонент выполняет определенную функцию и имеет специфический набор команд и сигналов управления, а так же принимаемых или отправляемых данных.

Использование гигагерцевого диапазона обусловлено появлением лидарной системы с ультраспектральным разрешением, оптический канал которой позволяет регистрировать сигналы с концентрацией близкой к фоновым значениям. Применение гигагерцевой полосы пропускания позволяет производить прием и обработку СКР сигнала наносекундной длительности без потерь. Произведен расчет параметров приемных устройств, необходимых для реализации гигагерцевого диапазона.

Создан облик аппаратной составляющей системы с использованием лабораторного стенда на базе PXI комплекса. Разработан программный комплекс по принципу модульной архитектуры, позволяющий производить регистрацию, обработку и хранение данных лидарных сигналов в реальном времени.

Основным результатом проделанной работы можно считать внедрение аппаратно-программного комплекса в реальный прототип авиационного лидара.

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

ПРЕДЛОЖЕНИЯ ПО РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА НА БАЗЕ ГИДРОМЕТЕОРОЛОГИЧЕСКОЙ СЛУЖБЫ ВС РФ

Необходимость создания в Вооруженных силах Российской Федерации (ВС РФ) автоматизированной информационной системы экологического мониторинга обусловлена тем, что они являются самостоятельной государственной структурой, деятельность которой в силу своего предназначения связана с риском вредных воздействий на окружающую среду (ОС), а также во многом зависит от состояния ОС. Влияние деятельности войск и сил флота на ОС разнообразно, а иногда уникально по факторам воздействия и характеру проявления. Разнообразный характер взаимодействия военных объектов с ОС требует комплексного подхода к оценке состояния экосистемы, включающей этот объект.

В соответствии с руководящими документами в современной структуре организации обеспечения экологической безопасности войск (сил) на уровне округа задачи по осуществлению экологического мониторинга возлагаются на экологические службы округов и региональные экологические центры (РЭЦ).Одной из серьезнейших проблем при развертывании региональных экологических центров является недостаток технических средств экологического мониторинга, отсутствие собственной сети наблюдательных постов экологического мониторинга, автоматизированных средств сбора, обработки и передачи информации по режимным и не режимным каналам связи Министерства обороны ВС РФ. Таким образом, налицо наличие противоречия между необходимостью проведения экологического мониторинга в ВС РФ и отсутствием возможности его проведения существующими силами и средствами, имеющимися на данный момент в распоряжении отдела экологической безопасности Департамента планирования и контроля материально-технического обеспечения МО РФ.

Решение данной проблемы путем разворачивания новой сети ведомственного экологического мониторинга и насыщения ее техническими средствами и личным составом представляется высоко затратным, трудноосуществимым и длительным мероприятием. Поэтому при проектировании сети ведомственного экологического мониторинга предлагается воспользоваться опытом создания Единой государственной системы экологического мониторинга (ЕГСЭМ). Начало ее созданию было положено в 70-х годах, когда в СССР была организована Общегосударственная служба наблюдений и контроля за уровнем загрязнения внешней среды (ОГСНК). Она функционировала на базе органов

Госкомгидромета и ряда других министерств и ведомств. На базе правопреемницы этой службы (Федеральной службы по гидрометеорологии и мониторингу окружающей среды) и сейчас осуществляются наблюдения за уровнем загрязнения атмосферы, водных объектов, почвы, биоты и проводятся сопутствующие гидрометеорологические наблюдения на территории Российской Федерации, за исключением территорий военных объектов.

Как видно из задач и структуры ЕГСЭМ, реализованной в основном на базе Федеральной службы по гидрометеорологии и мониторингу окружающей среды, при решении подобных задач в ВС РФ целесообразно возложить эти функции на аналогичную службу в Министерстве обороны РФ – Гидрометеорологическую службу (ГМС) ВС РФ.

Одним из элементов функционирования ГМС является проведение регулярных метеорологических, гидрометеорологических, аэрологических, гидрологических наблюдений на гидрометеорологических (метеорологических) станциях и постах гидрометеорологических (метеорологических) подразделений и частей. Наблюдения на разветвленной сети станций и постов осуществляются по единой программе, в одно и то же время одинаковыми техническими средствами.Гидрометеорологические станции и посты ГМС ВС РФ размещаются так, чтобы обеспечивалась необходимая точность интерполяции значений гидрометеорологических величин для пунктов дислокации частей и подразделений, в которых отсутствуют гидрометеорологические станции и посты.ГМС ВС РФ включает в себя гидрометеорологические подразделения видов и родов войск, расположенные по всей территории РФ в местах дислокации соединений и частей.

Таким образом, в настоящее время ГМС ВС РФ представляет собой организацию в составе Министерства обороны Российской Федерации, которая по составу сил и средств, своим возможностям после дооснащения соответствующими техническими средствами, методиками производства измерений и анализа полученной информации, способна решать задачи экологического мониторинга в местах дислокации соединений и частей ВС РФ.

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

МЕТОДИКА ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ НА ТЕРРИТОРИИ ПРОЕКТИРУЕМОГО ОБЪЕКТА СТРОИТЕЛЬСТВА

В настоящее время, когда реализуются масштабные строительные проекты, проблема прогнозирования состояния окружающей среды на территории объектастроительства еще на этапе его проектирования приобретает повышенную актуальность. Данная статья раскрывает суть методики, реализующей прогнозирование на основе экспертных оценок, метода анализа иерархий и материалов обоснования воздействия объекта на окружающую среду. Методика позволяет ранжировать опасность проектируемых объектов и присваивать им прогностические значения категории загрязненности окружающей среды в районе их размещения.

На начальном этапе формируется перечень возможных негативных влияний объекта или его отдельных площадок на окружающую среду.Далее предлагается отранжировать площадки объекта (источники) по степени потенциальной экологической опасности. В качестве исходных данных для такого ранжирования предлагается использовать материалыинженерно-экологических изысканий, обоснования воздействия на окружающую среду (ОВОС) проекты нормативов предельно-допустимых воздействий на окружающую среду, проектов"Перечень мероприятий по охране окружающей среды". Эти разделы входят в обязательный перечень проектной (эксплуатационной) документации объектов строительства (реконструкции), что исключает траты на дополнительные исследования.

В качестве критериев оценивания экологическая обстановка в районе будущего строительства выбраны пять категорий из Критериев оценки экологической обстановки территорий для выявления зон чрезвычайной экологической ситуации и зон экологического бедствия:относительно удовлетворительно; напряженная; критическая; кризисная; катастрофическая.

Обобщенные данные о воздействии объектов на окружающую среду сводятся к сведениям об объемах выбросов, сбросов, лимитов размещения отходов из материалов обоснования воздействия предприятия на окружающую среду и разработанного авторами показателя опасности загрязнения, базирующегося на показателях доли загрязнений с различными классами опасности выбрасываемых, сбрасываемых веществ и размещаемых отходов.

Из поставленной задачи – ранжирования проектируемых промышленных объектов по их воздействию на окружающую среду и присвоения им прогностических значений категории загрязненности окружающей среды в районе размещения, вытекает, что модель подготовки управленческого решения состоит из двух уровней: цель (ранжировать объекты) – критерии (объемы выбросов, сбросов, лимитов и показатели опасности) – альтернативы (категории экологической обстановки). Переход от ранжирования проектируемых объектов к оценкам категории экологической обстановки на их территории сводится к экспертным суждениям о категориях экологической обстановки на уже эксплуатируемых аналогах проектируемых объектов для самого опасного и

безопасного объекта. Дальнейшее деление объектов по категориям осуществляется согласно глобальным значениям величин приоритета метода анализа иерархий. Последующий анализ проводится в строгом соответствии с методом анализа иерархий для оценки 5-ти альтернатив по 2-м критериям, которые имеют количественные характеристики.

Методика прошла апробацию при проектировании объектов космодрома «Восточный».

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

МЕТОД СПЕКТРОСКОПИИ ЛАЗЕРНОЙ ИСКРЫ И ЕГО ПРИМЕНЕНИЕ ДЛЯ МОНИТОРИНГА ИСТОРИЧЕСКИХ ПАМЯТНИКОВ

Метод спектроскопии лазерной искры, известный за рубежом под аббревиатурой LIBS (от английских слов LaserInducedBreakdownSpectroscopy), предназначен для элементного анализа материалов. Он основан на исследования спектра вторичной эмиссии, возникающей в результате воздействия высокоинтенсивного лазерного излучения на исследуемый материал. При фокусировке пучка импульсного лазера с короткой (нано- или пикосекундной) в пятно диаметром 50-100 мкм на поверхности контролируемого объекта происходит образование факела плазмы, состоящей из ионов и электронов облучаемого материала и имеющей температуру десять-двадцать тысяч градусов. В излучении плазмы присутствуют характерные для данного материала атомные эмиссионные линии, которые могут быть зарегистрированы спектрометром. Анализ спектра излучения плазмы позволяет практически бесконтактно в режиме реального времени определять химический состав исследуемых материалов. Благодаря тому, что часть анализируемого материала испаряется в зоне обработки за время лазерного импульса, многоимпульсное воздействие позволяет проводить послойный анализ объектов.

Метод LIBS широко используется в промышленности, но в последние годы находит все более широкое применение для изучения памятников истории и культуры из металлов, камня, стекла, керамики и произведений живописи. Известные из научной литературы примеры таких применений метода LIBS относятся к практике музейной и реставрационной работы за рубежом, в нашей стране для аналогичных целей в настоящее время он не используется.

В данной работе в рамках сотрудничества со специалистами из Института прикладной физики (IFAC-CNR, г.Флоренция, Италия) нами были проведены исследования фрагментов скульптуры ангела из свинца с купола церкви Святой Екатерины, расположенной на Васильевском острове в Санкт-Петербурге. Было показано, что вLIBS-спектре поверхностного слоя данного памятника помимо свинца присутствуют частицы магния, железа, кремния и алюминия, которые являются характерными загрязнителями многих городских памятников, находящихся на открытом воздухе.

Результаты проведенных исследований позволяют рекомендовать метод LIBS для практического использования отечественным специалистам – реставраторам и музейным хранителям, – для мониторинга состояния экстерьерных памятников по месту их дислокации. Периодическое (например, 1 раз в 2-3 года) повторение LIBS-измерений позволит следить за динамикой процессов разрушения памятников и вовремя принимать решения о необходимости проведения реставрационно-консервационных мероприятий.

Другим перспективным применением метода LIBS в области сохранения культурно-исторического наследия может стать идентификация микроскопических грибов и других биологических поражений памятников, приводящих к их разрушению. Определение видового состава биопоражений можно проводить на основе создания базы данных опасных микроорганизмов. Важно то, что это можно также осуществлять в «полевых условиях», в том числе, включая такого рода измерения в программу мониторинга памятников. В настоящее время нами проводятся исследования возможности использования LIBS в этих целях. Результаты этой работы будут опубликованы позднее.

Рузанкина Ю.С., Васильев О.С., Вейко В.П., Гришканич А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

ПОВЫШЕНИЕ КОРРОЗИОННОЙ СТОЙКОСТИ ТРУБ НЕФТЕПРОВОДОВ МЕТОДАМИ ФОТОНИКИ

Проблема коррозии связана не только с повышением эксплуатационно-технической надежности и долговечности металлоконструкций, но и с проблемами экономически выгодного использования природных ресурсов и материальных средств. В последние годы остро ощущается ограниченность природных ресурсов, поэтому нерациональное использование этих ресурсов ставит под угрозу не только перспективы дальнейшего развития промышленности и сельского хозяйства, но и экологическое равновесие в природе. В предотвращении опасных последствий истощения природных ресурсов в борьбе с коррозией металлов отводится существенное место.

Существует множество вариантов по защите металлов от коррозии, но большинство из них малоэффективны. Были исследованы и предложены новые способы по защите металлов от коррозии за счет формирования оксидной поверхностной структуры. Работы проводились с применением волоконного иттербиевого лазера с длинной волны 1064 нм. Повышение коррозионной стойкости металлов можно осуществить при формировании на поверхности оксидных пленок, а также при снижении шероховатости поверхности. Для этого исследовались различные режимы и обработки поверхности стали и титана. Так как указанные процессы зависят от Тнагрева поверхности, то в процессе облучения осуществлялся контроль с помощью ИК-камеры.Для дальнейшего исследования облученной поверхности на коррозионную стойкость проводилась химическая обработка в кислоте. На месте коррозии происходит активная химическая реакция взаимодействия материала с окружающей средой или взаимодействие с иными поверхностями. Поставленная задача заключалась в том, чтобы данным методом компенсировать имеющиеся неровности материала, путём нанесения оксидной плёнки, которая более успешно выполнит функцию изначальной поверхности образца. Технология, исследуемая в работе, позволяет усовершенствовать методы повышения коррозийной стойкости, исключить некоторые стадии дополнительной обработки и пост обработки изделий и не наносит вреда окружающей среде.

Смирнов Л.В., Гришканич А.С., Кащеев С.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
ОАО «НПК «Государственный оптический институт им С.И. Вавилова»

ЛАЗЕРНЫЙ КОМПЛЕКС ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ ОБЪЕКТОВ ТЭК

Россия занимает весьма значительную территорию и практически на всей этой территории располагается большое количество объектов ТЭК. Одним из таких объектов является сеть нефти и газопроводов. Лишь используя новейшие разработки оптико-электронного приборостроения можно эффективно контролировать утечки из нефти и газопроводов.

Для обнаружения и своевременного устранения утечек были выбраны вещества индикаторы, что бы отследить детектируемые вещества. В качестве метода зондирования был выбран метод Комбинационного рассеяния. Полученные данные показали, что исследование лучше всего проводить на длине волны 266 нм. Была разработана структурная схема Рамановского лидара, проведен энергетический расчет, проведен расчет оптической системы, так же рассчитана масса приемного объектива и разработана его конструкция.

Фурина В.Н., Горохов В.Л., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

КОМПЬЮТЕРНЫЙ МОНИТОРИНГ И ОЦЕНКА БИОЛОГИЧЕСКОГО РАЗНООБРАЗИЯ И УСТОЙЧИВОСТИ ДРЕВЕСНЫХ РАСТЕНИЙ В УСЛОВИЯХ ГОРОДСКОЙ СРЕДЫ

Целью настоящего исследования является организация мониторинга и изучение видового состава местных и интродуцированных древесных растений озелененных территорий общего пользования города и их устойчивости к экстремальным факторам урбанизированной среды, что служит основой для выделения наиболее перспективных для озеленения видов.

Для достижения поставленной цели решались следующие задачи:

1. Осуществить мониторинг и изучение видового состава древесно-кустарниковых растений, определить их географическое происхождение.
2. Оценить биоразнообразие и жизненное состояние древесных растений в различных ландшафтно-функциональных зонах города.
3. Дать практические рекомендации по подбору видового ассортимента деревьев и кустарников.

Решение перечисленных задач предполагает использование методов «теоретической экологии» и методов экологического мониторинга, многомерного статистического анализа (корреляционный и регрессионный анализ).

В качестве объекта исследования выступают озелененные территории общего пользования (скверы, сады, бульвары, набережные, исключая насаждения парков и лесопарков).

Предмет исследования - анализ видового состава, оценка состояния и устойчивости древесно-кустарниковых растений в различных экологических условиях с учетом антропогенного прессинга.

Научная новизна работы. В рамках выполняемой НИР проведена инвентаризация скверов как одной из основных категорий озелененных территорий общего пользования, а также ряда садов и бульваров и определен видовой состав древесно-кустарниковых растений. Разработаны статистические основы подбора видового ассортимента деревьев и кустарников с учетом их

устойчивости для оптимизации городской среды и очистки атмосферного воздуха от загрязняющих веществ.

Практическая значимость НИР. Результаты исследования могут быть использованы для создания нормативов и стандартов по реконструкции и уходу за зелеными насаждениями.

Яковлев А.А., Рузанкина Ю.С., Кащеев С.В., Гришканич А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ ПО УСКОРЕННИЮ РОСТА СЕМЯН С ПОМОЩЬЮ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ

В настоящее время в мире наблюдается изменение климата и идет активный прирост населения. В связи со сложившейся ситуацией возникает необходимость по увеличению роста семян и созданию соответствующих условий. Изыскание новых методов для ускоренного роста семян является важной межгосударственной проблемой, так как существующие методы малоэффективны, дорогостоящи и многие из них опасны для человечества, так как химизация сельского хозяйства заключается в том, что после чрезмерного применения нитратов, фосфатов, пестицидов, синтетических регуляторов роста злой тенью следует отравление урожая, пищи и воды. Поэтому в настоящее время выбранная тема является актуальной, так как обусловлена необходимостью развития лазерных методов для решения проблемы по ускорению роста семян. Интерес вызван перспективой использования различных видов обработки семян в сельском хозяйстве с целью увеличения продуктивности растений и получения более высокого урожая.

Для решения задач по ускорению роста семян были исследованы и предложены новые способы по ускорению роста семян за счет лазерного воздействия. Внедрение новых технологий дает возможность стабилизации экологической обстановки на сельскохозяйственных угодьях, так как лазерная технология является экологически чистой и позволяет добиться результата без применения химических средств защиты растений. При использовании лазерного излучения семена сельскохозяйственных культур прорастают более активно под воздействием света с различными длинами волн. В результате лазерной обработки семян не только повышается урожайность зерновых культур, но и улучшаются сами свойства зерна. Все эти положительные достоинства позволяют рекомендовать лазерную технологию при выращивании сельхозкультур как в крупных, так и в мелких фермерских хозяйствах.

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения

КАРТИННАЯ ПЛОСКОСТЬ ФАСАДА

Всякое здание, внедренное в пространство биосферы, вносит дисбаланс в естественно-природные отношения. Условно говоря, городская среда это – многообразие параллелепипедов, состоящих из инородного вещества. И, эта суммарная инородная масса постоянно увеличивается, исчезает свободное пространство, важное для аудиовизуального восприятия. Кроме того, жители городов постоянно сталкиваются с ортогональной семантикой зданий, не несущей сведений о движении материи живой природы, что, крайне, необходимо для компенсации утраченных свойств.

Таким образом, возникают экологические проблемы для населения – нарушается информационная связь с окружающей средой, не хватает сведений о природных процессах внутри городского пространства. Необходима компенсация утраченных параметров среды.

На примере архитектурно – художественного оформления зданий Греции и Рима человечество получило опыт ордерной системы, который существенно повлиял на развитие технологий стилевого оформления зданий: барокко, классицизм,….

В естественно-природных условиях человека окружает световоздушное пространство, которое является благоприятным для аудиовизуального восприятия, а именно, для сосредоточения и рассеивания внимания. С точки зрения исторического опыта построения иллюзорного многоуровневого пространства в двухмерной плоскости картины, при рассмотрении художественного оформления фасадов, становится очевидным, что все богатство мира передается с помощью скульптурного рельефа на плоскость фасада и организуется в композицию по тем же правилам визуального восприятия, как плоскость картины или плафона. Сначала колонны выходили на первый план, затем они проецировались в пилястры с усеченными капителями и базами, которым отводилось место во втором пространственном уровне, потом в лопатки. Между пилястрами помещался низкий рельеф последнего плана.

Разнообразие медальонов, масок, декора давало возможность для переключения внимания.

Фактически, происходит анимация изображения колонны, проекции которой поочередно предстают перед зрителем в разных пространственных уровнях и растворяются в глубине перспективного пространства - плоскости фасада. Но при этом, возникают галереи и ниши, в которых прячутся скульптуры, вазы с цветами, т.е. опять, за счет преломления плоскости фасада, создается искусственная пространственная глубина с точками отсчета перспективного удаления. Информационное поле фасада здания строится по всем законам перспективы, аналогично построению композиционного пространства в классических образцах живописи.

Художественные решения фасадов, в результате, уже подготовлены для прочтения, также как тексты, произведения музыкальные, скульптурные, архитектурные и т.д.

Рассматривая, исторически сложившийся, видеоряд в архитектуре: Барокко, Классицизм, Модерн,… следует отметить, что архитектурный стилевой дизайн фасадов зданий изменяется следующим образом: обильно декорированный композиционные центры фасадов в барокко постепенно сменяется на все более скромные фасады классицизма и модерна. По мере уплотнения городского пространства, приближения зрителя к картинной плоскости фасада, изображения отступают по принципу снижения высоты рельефа, а именно: горельеф, барельеф, рельеф.

Любую плоскость - преграду человек стремится преодолеть и превратить в иллюзорное пространство.

Площадь фасада дробится (делится) на отдельные части. Система ризалитов, т.е. выступающих и уступающих плоскостей на фасаде здания также приводит к ощущению разных пространственных уровней, планов.

Исторически, архитекторы всегда применяли рельефный декор для моделирования иллюзорного, многоуровневого пространства в двухмерной плоскости фасада.

Архитектурный стилевой дизайн "растворяет" фасады и объемы зданий в городском пространстве,вносит информацию о естественно-природных процессах. И, это – мудрое решение экологических проблем, улучшает аудиовизуальное восприятие. Кроме того, адаптирует население к искусственно созданной городской среде с помощью формообразования, цвета скульптурных рельефов.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев А.В., Ушакова Н.П., Поленин В.И., Соловьев С.Н., Москаленко В.А.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля,судна

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ СУДНА: РЕЗУЛЬТАТЫ ПОДГОТОВКИ КОЛЛЕКТИВНОЙ МОНОГРАФИИ

Идея написания открытой коллективной монографии «Автоматизация процессов борьбы за живучесть корабля, судна» возникла сразу после того, как в ноябре 2012 г. в ОАО «Концерн «НПО «Аврора» в обеспечение комплекса работ по созданию ряда 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)».

Особая актуальность темы ни у кого не вызывала сомнений, так как интенсивное развитие информационных технологий и их широкомасштабное внедрения на кораблях ВМФ и судах Морского флота России обрели такие размеры, что стало принципиально необходимым в широком кругу специалистов, встретившись в комфортной обстановке, обсудить целый ряд накопившихся проблем.

Их появление было связано с необходимостью системно осмыслить не только открывшиеся новые широкие возможности современных информационных технологий, но на новом уровне и взвешенно оценить качественно новые возможности и роль главного элемента системы автоматизации – операторов в лице командиров кораблей и подводных лодок, капитанов судов, в том числе критического риска. Именно в их руки вместе с новыми информационными технологиями управления стали поступать средства с качественно новыми и критическими объёмами, содержанием и качеством используемой ими информации для принятия высоко ответственных управленческих решений.

С другой стороны, психофизиологические возможности человека и присущие ему наряду с возрастающими позитивными свойствами негативные субъективные свойства (так называемый «человеческий фактор») стали еще более значимыми для обеспечения безопасности эксплуатации сложнbых технических систем корабля, судно, а, тем более, при локализации аварийных ситуаций и аварий, управления борьбой за живучесть корабля, судна.

Более того, в результате проведенной Первой и последующих специализированных конференций по проблеме АП БЖКС, а также специализированного цикла научно-практических семинаров по обобщению лучших практик в этой сложной и широкой проблемной области, организация которых была возложена на специально созданное в 2012 г. Некоммерческое партнерство «Институт автоматизации процессов борьбы за живучесть корабля, судна», был накоплен весьма значительный и большой объем научных и практических данных.

Тем самым, целью написания предлагаемой читателям монографии и стала систематизация накопленных знаний по проблеме «АП БЖКС» с их классификацией для обеспечения процессов:

–теоретического обоснования анализа, синтеза и оптимизации процессов АП БЖКС, теоретического обобщения и обоснования практики создания, построения, освоения, эксплуатации и утилизации средств и технологий автоматизации процессов обеспечения безопасной эксплуатации (ОБЭ), локализации аварийных ситуаций и аварий (ЛА), борьбы за живучесть (БЖ) судов, в первую очередь, военного назначения (надводных кораблей (нк) и подводных лодок (пл) Военно-морского флота России и Военно-морских сил (ВМС) зарубежных государств), что и входит непосредственно далее в понятие БЖКС;

–научно-технического обоснования развития средств, систем и технологий АП БЖКС по её основным подсистемам (сегментам, кластерам) – подсистемам БЖКС в части обеспечения непотопляемости (Нс), взрывопожаро- и радиационной безопасности (Пс); живучести технических средств и оружия (Жс), защищенности экипажа судов (Зс) и управляемости (качества) системы автоматизированного управления БЖКС (Убс);

–обобщения и ранжирования лучших практик обеспечения БЖКС на основе систематизации данных и квалиметрического оценивания технологий БЖКС, оценки их конкурентной способности в интересах ускоренного практического освоения (инновационного обеспечения) лучших проектных и управленческих решений (ПУР) в части опубликованных данных в России и за рубежом в форме

изобретений, полезных моделей, книг, статей, докладов, отчетов о НИОКР и т.п., а также последующей их квалиметрической ранговой сертификации и аттестации объектов морской техники и морской инфраструктуры (ОМТИ).

Прикладная направленность представляемой коллективом авторов монографии обусловлена в этой связи необходимостью формирования коллективного мнения ведущих специалистов данной предметной области в части ряда проблемных вопросов, вошедших в следующие основные разделы:

1. История развития проблемы АП БЖКС.
2. Анализ публикаций по проблеме АП БЖКС.
3. Основные понятия проблемы АП БЖКС.
4. Методология исследования проблемы АП БЖКС.
5. Системные аспекты исследования проблемы автоматизации процессов БЖКС.
6. Специфические аспекты проблемы ап обеспечения БЖКС.
7. Автоматизация процессов обеспечения непотопляемости судов.
8. Автоматизация процессов обеспечения взры-вопожаро- и радиационной безопасности судов.
9. Автоматизация процессов обеспечения живучести технических средств и оружия кораблей и судов.
10. Автоматизация процессов обеспечения защищенности экипажей судов.
11. Автоматизация процессов обеспечения управления БЖКС.
12. Лучшие практики обеспечения АП БЖКС.
13. Ранговая партнерская сертификация средств и систем АП БЖКС и аттестация объектов морской техники и морской инфраструктуры.
14. Теоретические и практические проблемы развития технологий и систем АП БЖКС.

В докладе обсуждаются наиболее значимые и проблемные вопросы, вошедшие в презентуемую монографию, вопросы её структуры, наиболее значимые методологические вопросы.

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ТЕХНОЛОГИЯ СИНТЕЗА ФУНКЦИОНАЛЬНЫХ ПОДСИСТЕМ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ

Функциональная подсистема (ФП) – это совокупность информационных ресурсов (ИР) и информационных технологий (ИТ), обеспечивающих автоматизацию заданной функции управления на АРМ или на органе управления определенного уровня АСУ специального объекта ВМФ. ФП следует рассматривать, как информационный облик АСУ на трех уровнях: функциональном, системном и техническом. Функциональный уровень должен включать структурированный набор спецификаций функций управления, как для определенного АРМ, так и для органа управления, и требования к технологиям реализации функций. Системный уровень должен представлять управленческую совокупность сервисов и интерфейсов, определяющих прикладную платформу ФП. Технический уровень должен давать представление о ФП как программном продукте и идентифицировать структуру видов обеспечения ФП. Следовательно, ФП должна представлять собой совокупность унифицированных программных и информационных средств, функционирующих в среде унифицированных комплексов средств автоматизации (КСА), обеспечивающую автоматизацию заданной функции управления с использованием сервисов и базовых ИТ прикладных платформ КСА.

На основе изложенной сути ФП в докладе предложено построить методику ее синтеза из одиннадцати шагов:

1. определение назначения ФП и области ее использования в составе АСУ в защищенном исполнении специального объекта ВМФ;
2. выделение функций управления, которые должны быть автоматизированы (остальные выполняются пользователем вручную);
3. формулировка требований к процессу реализации автоматизированных функций управления;
4. выбор (разработка) прикладной платформы для КСА АРМ ФП;
5. формулировка требований к видам обеспечения реализации автоматизированной функции управления (АФУ);
6. разработка базовых безопасных (защищенных) информационных технологий, поддерживающих процессы реализации АФУ в ФП;
7. разработка приложений, т.е. комплексов информационных и расчетных задач, решаемых ФП с использованием базовых безопасных ИТ;
8. формулировка требований к структуре информационно-лингвистического обеспечения (ИЛО);
9. формулировка требований к специфической защите информационных ресурсов ФП;

10.макетирование базовых ИТ и приложений ФП;

11.разработка проекта ФП в целом.

Рассмотренная методика в целом соответствует общепринятой методике проектирования информационных систем, но имеет ряд особенностей. Первая, определение номенклатуры АФУ на конкретном АРМ должна осуществляться с использованием методов формализации при формулировке требований к реализации функций управления. Вторая состоит в выделении отдельного шага синтеза прикладной платформы КСА АРМ ФП с определением профилей базовых ИТ. Третья – это целесообразность разработки отдельных приложений уже после синтеза профилей базовых ИТ.

Для выполнения последовательности шагов предложенной методики рекомендуется использоваться соответствующие группы методов, а именно:

1. Методы выделения множества АФУ и формулировки требований к их реализации.
2. Методы проектирования прикладной платформы КСА АРМ ФП.
3. Методы проектирования базовых безопасных (защищенных) ИТ.
4. Методы проектирования ИЛО и прикладного программного обеспечения (ППО) в виде комплексов информационных и расчетных задач.

Первая группа методов должна быть направлена на определение, с помощью эталонных моделей функций управления, требований к этапам циклов управления, обоснование информационного взаимодействия ФП, входящих в состав АСУ специальных объектов ВМФ. Для решения названных задач должны последовательно применяться, во-первых, методы архитектурных и функциональных спецификаций, формирующих эталонные модели функций управления, и модели процессов функционирования ФП. Во-вторых, методы структуризации целей и задач. В-третьих, методы структурного анализа, обеспечивающие определение, на основе эталонных моделей функций управления, требований к этапам циклов управления. В-четвертых, методы обоснования алгоритмов реализации АФУ.

Вторая группа методов направлена на формирование функциональных требований к профилю ИТ ФП, создание модели интегрированной среды АРМ пользователя, разработку локального профиля базовой ИТ КСА АРМ ФП, формирование требований к архитектуре серверов приложений и, в итоге, на разработку проекта прикладной платформы ФП. Для решения названных задач необходимо последовательное применение методов архитектурных и функциональных спецификаций, методов структурного анализа, методов профилирования и методов разработки сценариев возникающих ситуаций управления.

Третья группа методов направлена на проектирование базовых ИТ путем формирования архитектуры серверов приложений, синтеза интерфейсов базовых ИТ, разработку математических моделей, на базе которых формируются базовые ИТ. Для решения этих задач необходимо последовательное применение методов разработки спецификаций архитектур, синтеза интерфейсов ИТ, разработка математических моделей объектов-оригиналов.

Четвертая группа методов направлена на проектирование ИЛО и ППО путем разработки проекта ИЛО, постановки и разработки алгоритмов информационных и расчетных задач, разработки проекта ППО.

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ПРИНЦИПЫ СОЗДАНИЯ ОБЩЕГО ИНФОРМАЦИОННОГО РЕСУРСА ВМФ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Современный этап развития автоматизированных систем управления (АСУ) характеризуется повышенной потребностью должностных лиц органов управления, взаимодействующих в рамках компьютерных сетей (КС), в актуальной, достоверной, своевременной и всесторонней информации, необходимой для качественного решения задач управления путем принятия целесообразных (результативных, эффективных, оптимальных) решений. В этой связи на первый план выходит проблема создания общего информационного ресурса (ОИР) ключевых структур, в том числе ВМФ, использование которого может обеспечить существенное повышение качества реализуемых информационных технологий во всех звеньях КС, а, следовательно, и качества принимаемых управленческих решений должностными лицами, как ВМФ, так и управляемых ими подразделений.

В настоящее время существует некоторый неавтоматизированный информационный ресурс (ИР), в том числе в органах управления ВМФ. Объективно этот ресурс используется неэффективно и не является общим, поскольку:

–отсутствуют единые правила и порядок описания, представления, формирования и использования этого ИР, а, следовательно, и обеспечения его защищенности;

–недостаточна оснащенность органов управления, действующих в рамках структуры, современными средствами автоматизации, телекоммуникации и связи и, что особенно важно,

современным программным и информационным обеспечением как для функционирования КС в целом, так и отдельных АРМ;

–несовершенны или вообще отсутствуют способы и средства доступа к этим ИР и механизмы управления доступом, управления его информационной защищенностью;

–нарушается принцип однократности ввода операторами АРМ оперативной информации;

–отсутствуют идентичность одинаковых ИР в органах управления;

–отсутствуют единые правила создания информационного продукта;

–отсутствует информационная совместимость, как в КС в целом, так и в отдельных входящих в нее локальных вычислительных сетях (ЛВС).

Основой ОИР в общем случае являются ИР, которые должны включать документы, определяющие реализацию процедур принятия управленческих решений (приказы, распоряжения, донесения, сводки и др.), нормативные документы (законы, подзаконные акты, нормы, штаты и т.д.), справочную информацию, учетную информацию (анкеты, картотеки), научно-техническую информацию, информацию, циркулирующую в КС (базы данных, файлы, сообщения), и другие массивы информации (фонды, схемы, плакаты и др.).

Сложность создания и внедрения ОИР обуславливается наличием большого количества различных источников и потребителей информации, их организационной и территориальной разнесенностью в рамках субъектов федерации. Кроме того, для системы управления структурными подразделениями характерна определенная динамика состава и содержания решаемых задач, возрастание в связи с этим информационных потребностей должностных лиц органов управления, а также большое количество неформализованной (неструктурированной) информации.

Ядром ОИР должно быть хранилище информации, которое представляет собой многомерные массивы, имеющие одинаковую структуру и содержащие интегрированную совокупность ИР, преобразованных (структурированных) по общим правилам хранения и защиты информации в ОИР.

В докладе авторами представлены три основные компоненты, которые должна включать система обеспечения ОИР, позволяющие в определенной мере продвинуться на пути решения названных проблем, включая:

1. Организационную, которая представляет совокупность органов управления (в том числе подразделений ВМФ), осуществляющих сопровождение ОИР. Такую компоненту необходимо создавать с учетом организационной структуры системы управления подразделениями ВМФ и подчиненными им подразделениями ВМФ.

2. Программную, являющуюся совокупностью программных средств, позволяющих осуществить актуализацию, поиск информации в хранилищах ОИР различного уровня, проведение ее анализа, контроля, обеспечение информационной безопасности ОИР.

3. Техническую, представляющую собой комплекс систем вычислительной техники, средств связи, телекоммуникационных систем, средств защиты информации и др., необходимых для ведения и использования ОИР.

Для решения всего комплекса задач по созданию ОИР в общем случае необходимо:

1. Обеспечить тесную кооперацию усилий органов управления, научно-исследовательских организаций и промышленных предприятий.

2. Кардинально пересмотреть методы, средства формирования, поиска, передачи, использования и защиты информации, применяемые при отсутствии как АСУ, так и ОИР.

3. Убедить руководство в том, что создание и внедрение ОИР в защищенном исполнении позволит в рамках КС обеспечить качественно новый уровень реализации информационных технологий на всех уровнях управления.

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ТЕХНОЛОГИЯ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ СРЕДСТВ И СИСТЕМ ОБЕСПЕЧЕНИЯИБ: МАСТЕР-КЛАСС

Анализ и синтез организационно-технических средств и систем обеспечения информационной безопасности (ИБ), в первую очередь, критических объектов, включая объекты морской техники и морской инфраструктуры (ОМТИ) в свете комплекса требований государственных, ведомственных и корпоративных регламентов по широкому спектру специализаций предусматривает объективную качественную и количественную оценку уровня обеспечения ИБ. Сегодня, в условиях решения национальной задачи обеспечения конкурентной способности и импортозамещаемости разрабатываемых технологий и систем обеспечения ИБ (СОИБ), это требование становится особенно актуальным и востребованным. И, прежде всего, в интересах концентрации национальных средств и компетенций специалистов при решении методологически и технологически сложных задач обеспечения защищенности современных систем автоматизации, противоборства в информационной сфере.

На пути решения этой проблемы к числу традиционно неоднозначных по эффективности задач относятся вопросы создания методологии и методик комплексной оценки и ранжирования уровня качества (квалиметрической оценки) обеспечения ИБ сложных эрготехнических систем (ЭТС). Более того, обеспечения объективности оценивания качества ОМТИ с использованием подобных методик. Так, даже по традиционным критериям оценивания конфиденциальности, доступности и целостности информационных ресурсов (ИР) ЭТС сегодня единых (с учетом инвариантности к специфике решаемых ЭТС задач) методик по существу нет. А, стало быть, нет условий для обеспечения ранжирования, оптимизации при альтернативном выборе и оценки конкурентной способности технологических решений (ТР). И это, при наличии целого ряда стандартов, руководящих документов и регламентов ФСТЭК.

С другой стороны, «непреодолимым» остается при проведении сертификационных и других видов испытаний ТР «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, автоматизированных систем в защищенном исполнении (АСЗИ) и СОИБ в целом. Это, естественно, с одной стороны, снижает мотивацию специалистов, а, с другой стороны, снижает в целом качество создаваемых СОИБ ОМТИ. Можно утверждать - приводит к неэффективному использованию национальных ресурсов (финансовых, трудовых, технических, материальных и др.). Но, самое главное, не позволяет обеспечить надежное технологическое развитие, конкурентную способность, устойчивое противостояние и противоборство в информационной сфере.

В последнее десятилетие на кафедре судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета разработан, освоен и успешно внедрён комплекс подобных методик и технологий, позволяющий в определенной мере решать круг данных задач.

В рамках доклада в формате мастер-класса среди них представлены и на базе накопленного опыта проведения курсового и дипломного проектирования, лабораторных работ и деловых игр продемонстрированы технологии использования программных комплексов поддержки квалиметрического оценивания, ранжирования и оптимизации свойств и характеристик средств и систем обеспечения ИБ в составе:

1. Программный комплекс (ПК) многокритериального квалиметрического оценивания и ранговой оптимизации проектных и управляющих решений (ПУР) «КРОПУР» (Реестр программ ФСИС № 2013612649, 11.03.2013/24.01.2013). ПК обеспечивает: оценку сводного (агрегированного) показателя качества (СПК, АПК) с соответствующими оценками свойств и групповых показателей качества (ГПК) АСЗИ в составе СОИБ ОМТИ по заданным значениям частных показателей качества (ЧПК) и ряду моделей предпочтений, включая 7 типовых моделей (простая, полная, бюджетная, системная, компромиссная, экономическая, полимодельная, лоцманская); многомерную визуализацию и регистрацию данных и ряд других сервисов.

2. ПК квалиметрического анализа и оценки конкурентноспособности технологических решений по информационной поддержке принятия решений судоводителем «QSWOT» (Реестр программ ФСИС № 2013612929, 18.03.2013/21.01.2013). ПК позволяет в экспресс-формате оценивать количественно (в отличии от традиционного SWOT-анализа) и сформулировать в сравнительном аспекте основные свойства разнородных ТР, включая системы информационной поддержки принятия ПУР судоводителями, а также уровня качества систем обеспечения ИБ.

3. ПК анализа, синтеза и оптимизации ПУР «АСОР». ПК обладает следующими дополнительными возможностями в сравнении с ПК «КРОПУР»: оптимизация параметров АСЗИ с использованием технологии корневой чувствительности; использование и актуализация баз данных и знаний по 30 лучшим альтернативным решениям в соответствующем классе средств и АСЗИ в целом.

4. ПК экспертного квалиметрического оценивания уровня качества технологических решений по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля, судна «МКО» (Реестр программ ФСИС № 2014613608, 31.03.2014/06.02.2014), в том числе в в версии ПК многокритериального экспертного квалиметрического оценивания средств и систем ОБИ «МКО-И». ПК обеспечивает: объективность производимых оценок ЧПК АСЗИ экспертами за счет создания условий их взаимной независимости в оценках; 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 процессов оценивания.

5. ПК многокритериального оценивания агрегированного показателя качества уровня ИБ АСЗИ разнородных объектов информатизации «АПК ИБ». ПК позволяет квалиметрически оценить конфиденциальность, доступность, целостность ИР АСЗИ в составе СОИБ с комплексной оценкой уровня ИБ ОМТИ по критерию АПК ИБ. Он обеспечивает: многокритериальную оценку ЧПК АСЗИ в соответствии с действующими регламентами, включая ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»; возможность учета специфики

аппаратных и программных средств при использовании методически инвариантного подхода; графическую визуализацию влияния свойств средств на их ГПК и АПК; информационно-справочную поддержку экспертов в части используемых терминов и их системной взаимосвязи.

Предложенные подходы и методики оценки качества АСЗИ в составе ОМТИ существенно снижают негативное влияние субъективного (человеческого) фактора при использовании принятых критериев и требований к качеству АСЗИ. Кроме того, позволяет ранжировать средства и СОБИ по интегрированному значению уровня качества, адекватнее оценить их роль и место в составе ОМТИ. А также - квалиметрически обоснованно решать задачи анализа, синтеза и оптимизации средств и СОБИ.

В дополнение к известным одним из новых конструктивных путей реализации названных возможностей, использования накопленного опыта и технологий комплексной оценки уровня ИБ ОМТИ авторы видят их применение в составе новой развивающейся системы ранговой партнерской сертификации (СПРС), как одной из реальных и перспективных в области комплексной оценки качества сложных ЭТС с их ранжированием и оценкой конкурентной способности. В том числе, в классе корабельных централизованных координирующих систем управления в защищенном исполнении, систем автоматизированной информационно-аналитической и интеллектуальной поддержки решений судоводителей, автоматических систем поддержки (оптимизации) решений и управления (АСПРУ) техногенными объектами повышенного риска, особенно, социально критичных и особо значимых систем.

Алексеев А.В., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ТЕХНОЛОГИЯ И ПРОГРАММНЫЙ КОМПЛЕКС МОНИТОРИНГА И УПРАВЛЕНИЯ ЗАЩИЩЕННОСТЬЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ

Информационная безопасность (ИБ) ресурсов предприятия является одним из важных направлений обеспечения комплексной безопасности предприятия. На сегодня исследован и систематизирован весьма широкий спектр типовых угроз и уязвимостей в информационных сетях разных уровней и задач. Федеральная служба по техническому и экспортному контролю непрерывно актуализирует банк данных угроз и уязвимостей, который насчитывает 182 и 11758 соответственно (по состоянию на 13.09.2015). Эти значительные числа говорят о том, что со временем, вероятнее всего, угроз станет только больше. Поэтому проблема непрерывного наблюдения за состоянием защищенности информационных ресурсов (ИР) компании (мониторинга защищённости ИР) от возможных угроз ИБ сегодня встает особенно остро.

В этой связи, как показывает практика, необходимо решить целый ряд проблем: разработать теорию и соответствующую технологию квалиметрического анализа, синтеза и оптимизации структур и алгоритмов комплексных систем ИБ по критериям конфиденциальности, доступности, целостность и их агрегирования в сводный показатель качества обеспечения ИБ объектов информатизации; перейти от традиционных средств класса IDS/IPS к постановке задачи и созданию средств анализа и предотвращения вторжений в реальном масштабе времени. Преимущественно с автоматическими алгоритмами функционирования и интеллектуальными подсистемами поддержки принятия решений администраторами безопасности на основе непрерывного измерения и наблюдения за динамикой системных показателей качества ИБ и, в первую очередь, агрегированного показателя качества (АПК).

С этой целью в интересах анализа состояния развития и специфических свойств технологий мониторинга защищенности ИР были протестированы демоверсии наиболее перспективных программных комплексов (ПК), включая «Symantec Endpoint Protection 12.1.6», «Kaspersky System Management», «ESET NOD32 Smart Security Business Edition 6.2», а также более ранние «XSpider 7.8», «Retina 5.14», «Microsoft Baseline Securite Analyzer 2.2», «Ревизор сети 2.0», «AppDetective 5.2.5», «Internet Scanner 7.0.2». Существенно различающиеся между собой по строение и функционалу, данные программные комплекса, к сожалению, не имеют общей системы оценки безопасности информационных ресурсов. Также ни один из этих ПК не обеспечивает оценку, контроль и мониторинг защищенности ИР по критерию АПК, а также общеизвестным критериям конфиденциальности, доступности, целостности.

В данном направлении сегодня уже достигнуты определенные результаты, включая: разработана технология анализа, синтеза, оптимизации проектных и управленческих решений (технология АСОР-ИБ), а также технология безизбыточного мониторинга АПК и других групповых показателей качества с полномасштабным комплексом информационно-аналитической и интеллектуальной поддержки принятия решений администратором ИБ (технология СПРУ-ИБ). Но, как правило, эти работы выполняются в инициативном порядке. В то время, как сложность задачи и её высокая наукоёмкость, необходимость комплексного решения задачи в формате мониторинга и управления защищенностью ИР предприятия требует концентрации усилий заинтересованных

сторон. Качественно новой возможностью данных технологий следует считать возможность автоматического представления администратору ИБ проектов управленческих решений, регистрации во времени и по содержанию принятых им решений; визуально наглядно производить ретроспективный анализ эффективности управления ИБ.

В докладе представлены достаточно новые принципы и технологические решения построения комплекса мониторинга и управления защищенностью информационных ресурсов предприятия на основе ПК «СПРУ-ИБ». Они включают квалиметрическую оценку ИБ по критерию агрегированного показателя качества (СПК) с предварительной оценкой групповых показателей качества (ГПК) путем многокритериального полимодельного оценивания конфиденциальности, доступности, целостности. Рассмотрены ключевые вопросы технологической реализации технологии СПРУ-ИБ и приведены результаты их опытной отработки

Важной особенностью разработанной и принятой в ПК «СПРУ-ИБ» (в форме макетного действующего образца, в том числе с вариантом web-реализации) архитектуры и комплексного алгоритма функционирования является их инвариантность к специфике решаемых задач. Это позволяет при наличии у предприятия соответствующих регламентирующих и нормативно-методических документов достаточно оперативно (в течение (1,5…2,0) месяцев) и бюджетно (малозатратно) адаптировать его к реальным условиям функционирования.

Рассмотрены ключевые вопросы технологической реализации сформулированных принципов и приведенные результаты их опытной отработки, подтвердившие перспективность предложенных качественно новых технологических решений по обеспечению высокоуровневой защиты информационных ресурсов предприятий.

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

СОВРЕМЕННАЯ ТЕОРИЯ ОПТИМИЗАЦИИ ИНФОРМАЦИОННОЙ ИЗБЫТОЧНОСТИДИСКРЕТНОГО ПРЕДСТАВЛЕНИЯ ПРОЦЕССОВ ПРИ МОНИТОРИНГЕ И УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

В 2015 году исполнилось 100 лет, как E.T. Whittaker сформулировал впервые закономерность, вошедшую позже в историю науки, как теорема отсчетов Уиттекера-Котельникова-Шеннона (УКШ). И до настоящего времени эта закономерность играет весьма большую роль в математике, физике, технике, оптике, кристаллографии, других областях, включая мониторинг и управление информационной безопасностью объектов морской техники.

Дискретизация сигналов и процессов практически любой природы во времени в сочетании с их квантованием по уровню лежит в основе их цифровой обработки. Несоблюдение условий теоремы УКШ является крайне критичным и сопровождается либо неадекватным преобразованием данных с соответствующими погрешностями и ошибками, либо необоснованным введением информационной избыточности с соответствующим завышением требований по составу средств, их качеству и ресурсным затратам. Данную угрозу информационной безопасности нельзя нидооценивать, так как ошибки выбора параметров преобразования приводят к существенным и необратимым погрешностям, потери целостности информации и доступности к её содержательной части.

Оптимизация выбора частоты дискретизации исходных процессов и сигналов позволяет обеспечить компромиссные условия между этими противоречивыми факторами, что и является одной из ключевых задач на пути аналого-цифрового преобразования данных и их последующей обработки. Специфика преобразования и обработки информации, как и особенности преобразовываемых исходных процессов и сигналов, должны непосредственно учитываться при дискретизации. Но именно это и определяет сложность проблемы выбора её параметров.

Поэтому многие годы от первой формулировки условий и требований к выбору значения частоты отсчетов в 1915 г. E.T. Whittaker, в 1927 г. W.L. Ferrar, в 1928 H. Nyquist, в 1929 г. J.M. Whittaker, в 1933 Котельниковым В.А., в 1946 D.Gabor и в 1949 К. Шеннономочень многие авторы всесторонне исследовали эту проблему. Делали и продолжают делать попытки обобщения этого базового параметра цифрового преобразования информации – частоты выборки отсчетов, частоты дискретизации процесса.

Следует особо отметить, что данную закономерность В.А. Котельников в 1933 г.сформулировал в форме не одной, а семи теоремотсчетов. Более того, в пятой теореме был рассмотрен наиболее общий вариант представления функции, имеющей ненулевую нижнюю частоту. Случай дискретизации сигналов - не по верхней граничной частоте спектра, а по его полосе частот. Парадоксально, но этот обобщенный вариант теоремы УКШ мало знаком сегодня даже специалистам. Это часто приводит, особенно при полосовых сигналах, к неоправданному завышению избыточности, а в ряде случаев даже к ошибочному выбору параметров их дискретного представления и, естественно, к соответствующим необратимым погрешностям.

Сразу следует отметить, что представить полный ряд авторов в этой области вряд ли возможно, так как за прошедший 100-летний первый период развития теоремы и теории отсчетов этот ряд исследователей представляется весьма и весьма обширным. В то время, как в первую очередь, конечно, представляет интерес именно история развития самой теоремы отсчетов.

В докладе на основе спектральной интерпретации физических процессов выборки сигналов при их дискретизации, анализа природы формирования сигнальной и информационной избыточности представлено малоизвестное обобщенное выражение теоремы отсчетов для реальных полосовых сигналов с конечной (неидеальной) крутизной наклона спектра вне его рабочей полосы (УКШр). Минимизация погрешностей преобразования и обработки сигналов, данных, информации в целом сегодня, безусловно, должна рассматриваться в системно целостном процессе анализа, синтеза, оптимизации. И именно только такой подход может обеспечить обоснование проектного, управленческого решения и минимизацию риска заказчика при решении этой традиционной, но далеко не однозначной задачи.

Таким образом, несмотря на пройденный 100-летний рубеж освоения тайн дискретного преобразования временных функций и закономерностей их представления массивом выборочных значений, природа этих процессов продолжает привлекать внимание большого круга исследователей. Как математиков, среди которых E.T. Whittaker впервые сформулировал теорему отсчетов в виде кардинального ряда, так и технических физиков, связистов, теоретиков и практиков современной информатики и кибернетики, исследователей современных информационных технологий и многих других смежных дисциплин.

В результате проведенных исследований и формулирования закономерности дискретного представления информации в виде теоремы УКШ в практику цифровой обработки данных сегодня надежно вошли рекомендации, учет которых позволяет корректно переходить к ограниченным массивам данных и, тем самым, минимизировать информационную, функциональную, структурную, алгоритмическую и другие виды избыточности.

Сегодня, даже с учетом целого ряда ограничений, диктуемых особенностями практической реализации теоремы УКШ, знание закономерностей дискретного преобразования данных позволяет использовать для полосовых сигналов в области МГц-частот и выше кГц-частоты дискретизации с соответствующим выигрышем в $k \geq 10 \ldots 100$ раз и более.

Безусловно, это имеет особое значение для объектов морской техники и морской инфраструктуры, где ведется традиционная борьба за каждый ресурсный показатель, а упускать названные возможности вряд ли можно считать допустимым.

Это, тем более, важно при минимизации объема данных, выводимых операторам на экраны мониторов объектов морской техники, особенно, в критических условиях выявления и нейтрализации угроз безопасности, соответствующих информационных инцидентов.

Наконец, даже в условиях освоения революционных возможностей современных информационных технологий с терабитными возможностями элементной базы вопросы информационной избыточности продолжают оставаться актуальными. И не только актуальными, но и критичными в связи комплексом новых ограничений по обработке информации, обусловленных принципиальным ограничением психофизиологических возможностей операторов по визуальной, интеллектуальной, групповой обработке данных, представляемых для принятия соответствующих проектных и управленческих решений.

В этих условиях именно максимизация ценности представляемых и обрабатываемых данных, включая удельную ценность на каждый бит данных, их системную значимость в интересах качества принятия решений предъявляет жесткие требования к методической корректности и повышенной точности выбора каждого из параметров обработки сигналов. Именно такую возможность предоставляет рассмотренный математический аппарат и методика обобщенного дискретного представления реальных полосовых процессов в соответствии с теоремой отсчетов УКШр и оптимизации информационной избыточности в целом.

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АЛГОРИТМ ОЦЕНКИ АГРЕГИРОВАННОГО ПОКАЗАТЕЛЯ КАЧЕСТВА ОБЕСПЕЧЕНИЯ ИБ

Анализ, синтез и оптимизация систем обеспечения информационной безопасности (ИБ) объектов морской техники и морской инфраструктуры (ОМТИ) в свете современных требований регламентирующих документов по широкому спектру специализаций неизбежно предусматривает необходимость объективной (согласованной сообществом специалистов и органов управления) качественной и количественной оценки уровня ИБ ОМТИ.

Тем не менее, широко признанных моделей и сертифицированных программных средств их реализации сегодня, к сожалению, практически нет. В этом контексте обсуждение различных вопросов оптимизации систем обеспечения ИБ (СОИБ) различных объектов автоматизации, включая

ОМТИ, представляется мало конструктивным и, тем более, не имеющим обозримых временных границ.

В этой связи руководствуясь известной концепцией полимодельного оценивания, анализа, синтеза и оптимизации современных сложных организационно-технических систем, в докладе представлены результаты систематизации методов агрегирования векторных критериев и оптимизации решений, ранее приведенные в журнале «Морские интеллектуальные технологии» (№ 2 (28) Т.1, 2015, с. 51).

Их сравнительный анализ с учетом опыта многочисленных многокритериальных оценок, в том числе при решении различных исследовательских и проектных задач применительно к ОМТИ, показал, что наиболее предпочтительным следует считать так называемый метод гармонической оптимальности (МГО).

К числу преимуществ МГО следует относить его «компромиссное положение» в части получаемых оценок при агрегировании векторных критериев между методом равномерной оптимальности (МРО) с аддитивным алгоритмом свертки частных показателей качества (ЧПК) и методом справедливого компромисса (МСК) с мультипликативным алгоритмом свертки.

В частности, при этом исключаются, как недостаток МРО (увеличенная погрешность оценивания (завышение оценок) при нулевых значениях хотя бы одного из ЧПК), так и недостаток МСК (заниженные оценки во всем диапазоне значений ЧПК).

В докладе приведены алгоритмы оценки агрегированного (сводного, интегрального, обобщенного, генерального и т.п.) показателя качества (АПК) и ряд характерных примеров. Приведенные данные наглядно, по мнению автора, демонстрируют перспективность перехода от традиционно используемого МРО с аддитивным алгоритмом свертки ЧПК к МГО с гармоническим (аддитивно-мультипликативным) алгоритмом свертки ЧПК.

Названное преимущество МГО представляется особо ценным при выполнении многовариантных оценок качества ОМТИ, включая оценки уровней ИБ с использованием групповых показателей качества (ГПК) типа конфиденциальность, доступность, целостность информации.

Еще более значимо данное преимущество МГО при полимодельном вариантном анализе качества обеспечения ИБ ОМТИ, т.к. за счет «промежуточного положения» получаемых оценок АПК между оценками, получаемыми с использованием МРО и МСК, позволяет «объективнее» (без критичных выбросов) сравнивать разнородные объекты анализа и, тем самым, «не упускать» (не исключать) из анализа те свойства ОМТИ, которые не всегда могут быть полномерно оценены с использованием выбранных ЧПК и ГПК.

Конечно, более строгая аргументация выбора метода агрегирования возможна и целесообразна. Но в данном контексте и до рассмотрения условий конкретной задачи может быть принята вполне достаточной, так как аксиомой многокритериального оценивания, анализа, синтеза и оптимизации, как известно, является приоритет лица, принимающего решение (ЛПР). Причем, как при выборе системы критериев, их метрики, так и «особого (эксклюзивного) права» ЛПР при регуляризации задачи оптимизации и, непосредственно, при выборе решения об оптимальном варианте решения задачи.

Алексеев А.В., Ливанов И.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

WEB-РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ СПРУ ДЛЯ РУКОВОДИТЕЛЕЙ ОМТИ

Одной из перспективных технологий поддержки принятия проектных и управленческих решений, соответствующих систем информационной поддержки лиц, принимающих решения (ЛПР), становится и в последнее время активно развивающаяся технология СПРУ – систем (информационно-аналитической и интеллектуальной) поддержки (проектных – для лиц, обосновывающих (ЛОР) и исполняющих (ЛИР) решения, управленческих решений – для ЛПР) решений и управления (доведения принятых решений до ЛОР и ЛИР, их регистрации, мониторинга обстановки, принятия корректирующих решений и т.д.).

Технология СПРУ (ФСИС, № 2014614620, 29.04.2014 / 05.03.2014), первоначально разработанная для решения задач информационной поддержки руководителей морских объектов повышенного риска (старших механиков, капитанов танкеров и т.п.) для обеспечения их безопасной эксплуатации (ОБЭ), локализации аварийных ситуаций и аварий (ЛА) и борьбы за живучесть (БЖ), была в развитие полученных результатов адаптирована к решению задач ОБЭ, ЛА и БЖ командирами БЧ-5 кораблей и подводных лодок, а также соответствующих ЛПР в составе учебно-тренировочных центров.

Далее, с учетом выявленной инвариантности разработанной технологии к специфике решаемых задач, были рассмотрены и разработаны варианты адаптации технологии СПРУ к задачам поддержки решений администратора безопасности информационно-коммуникационных сетей, операторов (по специализации) центров управления кризисными ситуациями, операторов центров

экологической безопасности города-области-региона, а также даже ЛПР в звеньях управления городским хозяйством, глав муниципальных образований, администрации районов и городов.

При этом, отработка вариантов адаптации предусматривает:

–анализ и структурирование (при необходимости) целей и решаемых задач соответствующим органом управления на основе обеспечения строгого соответствия действующих положений об органе управления и другой нормативно-методической (НМД), организационно-распорядительной документации (ОРД) и регламентов;

–формирование системы соответствующих критериев и показателей качества элементов и органа управления в целом, включая частные (ЧПК), групповые (ГПК), модельные (МПК) показатели качества и агрегированный (сводный, обобщенный, интегральный, генеральный и т.п.) показатель качества (АПК);

–формирование и актуализация базы данных и знаний (БДЗ) в стартовой комплектации на основе систематизации и цифровизации лучших практик управления соответствующих звеньев и органа управления в целом;

создание и экспериментально-опытная отработка пилотного контура управления (ПКУ) с его последующим масштабированием и запуском в эксплуатацию СПРУ в целом для соответствующего органа управления с последующей его аттестацией, сертификацией соответствия и сертификацией качества разработанных средств и СПРУ в целом.

Для обеспечения оперативности развертывания, мобильности и устойчивости создания, освоения и функционирования элементов и СПРУ в целом была поставлена и решена задача web-реализации сетевого взаимодействия элементов СПРУ. В результате формирования архитектуры и соответствующих настроек были проведены испытания сетевой реализации СПРУ в составе: сервера БДЗ (ноутбук), двух стационарных автоматизированных рабочих мест (АРМ) для администратора СПРУ и оперативного дежурного СПРУ, мобильных АРМ (смартфоны, планшеты) для операторов (ЛОР) органа управления и ЛПР. При этом, функции всех АРМ были взаимно заменяемыми.

Данный вариант реализации технологии СПРУ предоставляет возможность ТОР-руководителям непрерывно, мобильно и практически объективно контролировать текущее состояние объекта управления по системным показателям качества АПК, МПК и ГПК, причем, в 2-х битовой шкале контроля по 4 основным состояниям: ВТ (зеленая индикация) – выполняются требования (показатели качества, например, в диапазоне значений (90…100)%); УНТ (оранжевая индикация) – угроза невыполнения требований с диапазоном значений (80…90)%; НТ (красная индикация) – невыполнение требований с диапазоном значений (50…80)%; ПУ (серая индикация) – потеря управления с диапазоном значений менее 50%.

Как показывает опыт, важным практическим следствием перехода к технологии СПРУ следует считать актуализацию в процессе освоения технологии СПРУ работ по совершенствования (как правило, упрощению) структуры органа управления, его ОРД, НМД и других регламентов с целью оптимизации избыточности (как возможности минимизации без потери системного качества по уровню АПК), обеспечения «прозрачности» управления в интересах повышения его результативности и качества.

Баркова Н.А., Грищенко Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЗАЩИТНОГО МОНИТОРИНГА СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ

Стационарные системы защитного мониторинга по вибрации широко используются во многих отраслях промышленности и на транспорте в качестве средства повышения надежности и эффективности управления роторным оборудованием. Достоверность и оперативность принятия решения являются основными критериями эффективности таких систем, т.к. зачастую принимать правильное решение необходимо за считанные секунды до возникновения опасных ситуаций с необратимыми последствиями. Поэтому повышение достоверности определения состояния, в том числе и в переходных режимах работы, и минимизация времени принятия решения является крайне актуальной задачей при разработке таких систем. Подобные системы могут эффективно использоваться и в качестве средства информационной поддержки при управлении оборудованием, предоставляя оператору информацию о нежелательных режимах работы и о последствиях таких режимов.

В простейших системах, обеспечивающих аварийную защиту оборудования основным параметром для принятия решения является нормируемая стандартами интегральная низкочастотная вибрация. Реализация таких систем относительно проста и не требует создания сложных алгоритмов обработки данных. При этом достоверность таких систем ограничена, т.к. низкочастотная широкополосная вибрация характеризует опасность вибрации для самого агрегата, но не отражает в достаточной мере связь с его техническим состоянием. Некоторое повышение

достоверности идентификации состояния в подобных системах может быть достигнуто путем увеличения количества точек контроля и измерения характеристик других рабочих процессов. Однако опыт разработки и внедрения подобных систем показывает, что качественное повышение эффективности достигается за счет внедрения технологий мониторинга и оперативного диагностирования на основе широкой номенклатуры измеряемых параметров. Внедрение подобных технологий предполагает решение целого ряда задач.

Во-первых, необходимо извлечь из вибрации как можно больше информации, характеризующей различные физические процессы. Для этого вибрацию разделяют на компоненты разной природы – периодические, случайные и импульсные. Каждая из таких выделенных компонент связана с изменением свойств различных физических процессов. К примеру, рост периодических компонент связан с увеличением энергии колебательных процессов, рост случайных компонент - с изменением сил трения и характером взаимодействия сред, а появление импульсных компонент характеризует возникновение ударных взаимодействий.

Во-вторых, для эффективного мониторинга следует внедрять алгоритмы оптимальной адаптации пороговых значений. Здесь следует учитывать изменение вибрации агрегата не только из-за изменения режима, но и учитывать флуктуации внешних условий – изменение температуры объекта в процессе прогрева, изменения температуры окружающей среды и т.п. Одним из эффективных способов адаптации пороговых значений является накопление и анализ данных в блоках (накопителях) различной длительности по времени и расчёте порогов для каждого такого накопителя отдельно на основании определения базового значения по следующему накопителю (большему по длительности). Это дает возможность абстрагироваться от медленных изменений параметров и повысить чувствительность идентификации причин изменения состояния, которое может происходить с различной скоростью.

В-третьих, для повышения эффективности технологий постановки оперативного диагноза необходимо переходить от поузловой диагностики к диагностированию объекта в целом, что требует от разработчиков таких систем тонкого понимания связи дефектов конкретного узла с широким перечнем выделенных из вибрации компонент во всех измеряемых на агрегате точках.

Важнейшей задачей при построении систем защитного мониторинга является обеспечение контроля состояния в переходных режимах работы, ведь именно в таких режимах происходит большинство аварий. Вопросы контроля и мониторинга в подобных режимах решаются путем повышения порогов на заданные величины. Диагностирование в переходных режимах в большинстве систем не предусмотрено из-за проблем в получении необходимой информации – параметров гармонических рядов. Решить данную проблему можно путем создания устойчивых методов выделения информативных гармоник из спектров вибрации при нестабильной частоте вращения, основанных на анализе мгновенных неусредненных спектров с подходящим для конкретной нестабильности частотным разрешением, а также путем анализа широкополосных спектров.

В качестве примера современных систем защитного мониторинга, построенных с учетом перечисленных способов повышения эффективности, можно привести судовую бортовую стационарную систему диагностики, созданную с участием авторов и переданную для использования на кораблях с атомными энергетическими установками. Гражданский вариант системы показал свою эффективность на одном из промышленных предприятий Санкт-Петербурга.

Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

АНАЛИЗ ОПЫТА ОРГАНИЗАЦИИ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИЯ КАЧЕСТВА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

В условиях реализации мер по переходу России к устойчивому социально-экономическому развитию создаваемые сложные эрготехнические (человеко-машинные) комплексы и системы (ЭТС) для объектов морской техники (ОМТ) должны быть, прежде всего, конкурентоспособными. Важнейшая особенность современного этапа развития систем управления состоит в том, что всё большее значение приобретает адекватный учёт факторов их сложности и информационно-технической насыщенности и, прежде всего, их комплексного качества. Особенно ярко это проявляется в отношении объектов повышенного риска, включая суда с атомными установками, супертанкеры, химовозы, стационарные ледостойкие морские платформы и другие.

В этих условиях именно конкурентоспособность автоматизированных систем (АС) ОМТ, как возможность превзойти конкурентов в заданных условиях, с учетом национальных интересов по обеспечению технологической независимости от мировых лидеров, следует рассматривать как важнейший системный критерий, системообразующий фактор. Более того, как саморегулирующий механизм и соответствующий «рычаг» управления качеством АС ОМТ, а также как один из важных маркетинговых аргументов.

Анализ тенденций и проблем развития систем оценки качества современных автоматизированных систем (АС) ОМТ и, в целом, сложных эрготехнических систем (ЭТС), а также их сертификации и аттестации показывает, что никакие эпизодические и системно разрозненные мероприятия не могут обеспечить устойчивое улучшение качества современных ЭТС, а тем более высокий (требуемый, прогнозируемый) уровень конкурентной способности ОМТ.

В качестве одного из перспективных направлений обеспечения конкурентоспособности создаваемых систем автоматизации в условиях назревшей необходимости обеспечения реальной конкуренции национальных продуктов и услуг на международном рынке можно рассматривать концепцию и соответствующую ей технологию ранговой партнерской сертификации и аттестации объектов различного назначения (РПС), основные положения которой были изложены ранее. Прежде всего, это актуально для тех объектов информатизации, для которых сертификация качества наиболее востребована с учетом условий интенсивного развития технологий и систем автоматизации.

Анализ накопленного опыта показал, что именно полная автоматизация процедур обработки результатов анонимного и безличного экспертного оценивания при коллегиальности принятия экспертным советом решения о сертификации АС и аттестации ОМТ позволяет:

– с одной стороны, принципиально упростить процедуру принятия решений (только по времени цикл прохождения заявки на сертификацию сокращается с 6 и более месяцев до 10-12 и менее дней), в том числе за счет использования web-технологий и электронного документооборота;

– с другой стороны, практически полностью исключить при реализации концепции РСА негативное влияние человеческого фактора и других субъективных факторов.

В сравнении с действующей системой сертификации соответствия предложенная система сертификации качества АС обеспечивает, прежде всего, прогрессивное саморазвитие системы партнерской ранговой сертификации за счет обеспечения условий равной конкуренции для участников, ориентированной на квалиметрическую оценку качества и ранжирование технологических преимуществ.

В результате сертификационных испытаний семи заявленных ТР Центром РПС (в состав ПЭС вошло 11 специалистов при среднем значении индекса квалификации ИКэс=52,9) было принято решение (коэффициент вариации оценок экспертов не превысил КВ=13,7%, что следует считать вполне приемлемым) о выдаче сертификатов качества по трем из них с соответствующими рейтингами по отношению к национальному и мировому уровням качества технологического развития Rм/Rн соответственно 3/1, 4/2, 8/5. В целом полученные результаты подтвердили весьма высокий уровень технологического совершенства и конкурентной способности заявленных на РПС отечественных ТР, позволили партнёрам определить ближайшие цели по их совершенствованию и развитию, достижению высоких конкурентных уровней.

Так, в результате экспертизы программных комплексов (ПК) в классе средств информационной поддержки принятия решений (СИП) при проектном обосновании надежности, живучести и устойчивости сложных организационно-технических систем, включая ОМТ, автору ПК «Арбитр» профессору Можаеву Александру Сергеевичу (компания ОАО «СПИК СЗМА») был вручен сертификат качества № СК.0002 от 05.12.2013 с ранговым номером Rм=1 по отношению к мировому уровню технологического развития систем названного класса.

Понятно, что точность производимых оценок и, особенно, рейтинговых показателей непосредственно определяется составом и содержанием баз данных и знаний (БДЗ) по альтернативным ТР соответствующего класса средств и услуг. Вместе с тем, именно необходимость непрерывной актуализации БДЗ альтернативных ТР (их развития) при подготовке разрабатываемых изделий к РПС стимулирует и координирует проведение патентных исследований, повышает эффективность проведения аналитических и маркетинговых исследований в соответствующей предметной области. Более того, соответствующую квалиметрическую оценку и мониторинг альтернативных ТР на рынке следует рассматривать, как важный когнитивный источник данных проектирования. Это, в свою очередь, является весьма положительным фактором развития предприятия, наращивания его научно-технического потенциала.

Представленный опыт организации и проведения открытых (публичных) заседаний партнерских экспертных советов по рассмотрению результатов автоматического информационно-аналитического обеспечения экспертного оценивания и формирования отчетных документов, включая сертификаты качества (в отличие от традиционных сертификатов соответствия) и формируемые реестры средств, сертифицированных в системе РПС, в целом подтвердили перспективность предложенной концепции и путей её реализации.

Выводы и рекомендации. Сегодня, при наличии определенных сложностей в решении проблемы повышения технологического уровня создаваемых технических комплексов и систем, обеспечения их конкурентоспособности, в качестве одного из перспективных путей и способов решения данной проблемы следует рассматривать переход к предложенной концепции и технологии РПС ЭТС и, особенно, критических ЭТС, включая ОМТ.

Накопленный опыт реализации концепции, теории и практики добровольной ранговой партнерской сертификации качества изделий и услуг в рамках некоммерческих квалификационных обществ и партнёрств за счет информационно прозрачных технологий количественного оценивания качества сертифицируемых изделий и услуг позволяет создать равные условия участникам рынка для прогрессивного развития предприятий и отраслей промышленности в целом.

Как следствие, это позволяет оптимизировать организационно-технические процедуры, мотивировать и существенно ускорять организацию и создание конкурентоспособных эрготехнических комплексов и систем, в том числе, автоматизированных систем управления объектов морской техники и инфраструктуры.

Бучина Д.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

КРИТИЧЕСКИЕ УГРОЗЫ И УЯЗВИМОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Облачные технологии, как известно, представляют собой процедуры и процессы реализации способа работы с данными, при которых компьютерные ресурсы представляются в виде онлайн-сервиса. «Облако» в данном определении означает наличие сложной распределенной компьютерной инфраструктуры.

Согласно определению Международной некоммерческой ассоциации специалистов в области электротехники (IEEE), главного разработчика стандартов по радиоэлектронике и электротехнике, облачные технологии – это «парадигма, которая постоянно хранит пользовательскую информацию на интернет-серверах и лишь временно кэшируется на стороне пользователя». Со стороны клиента облачные технологии могут использоваться посредством стационарных и мобильных компьютерных систем, в том числе ноутбуков, смартфонов, планшетов.

При этом, безопасность хранения и пересылки данных является одним из самых основных вопросов при работе с облаком, особенно в отношении конфиденциальных, приватных данных.

Вдокументе “Cloud Computing Security Risk Assessment. Benefits, risks and recommendations for information security”, разработанномагентством European Network and Information Security Agency (ENISA), систематизированыосновныерискииуязвимостиоблачныхсредспозициипользователей (критическиеугрозыиуязвимостиоблачныхтехнологий):

–привязка к одному облачному провайдеру, без возможности легко его изменить;

–ошибки изоляции и разграничения доступа между ресурсами в облачной архитектуре, из-за чего возможны утечки данных;

–нарушения требований национальных законодательств в связи с использованием облачных сред;

–действия злоумышленников из числа привилегированных (лигитимных) сотрудников облачного провайдера;

–неполное удаление данных в облачной инфраструктуре.

Так же наиболее характерными угрозами для облачных технологий специалистами по сетевым технологиям часто называются:

–DDoS-атаки на сетевую инфраструктуру между облаком и клиентом;

–перехват аутентификационных данных для доступа к облаку через облачные API;

–перехват данных, отправляемых и получаемых из облака;

–использование уязвимостей для получения несанкционированного доступа к данным другими пользователями облака;

–нарушение изоляции среды, предоставленной клиенту в рамках облачной услуги;

–атаки на клиентские браузеры;

–плохую очистку клиентской информации на стороне провайдера облачных услуг.

Для анализа угроз и уязвимостей облачных сред были рассмотрены наиболее популярные облачные хранилища данных: Dropbox, Google Drive, Яндекс.Диск, SpiderOak. Полученные оценки и пути нейтрализации критических угроз вынесены на публичное обсуждение и анализ.

О критичности использования используемых сегодня облачных технологий говорит также факт принятия государственных решений в части защиты интересов пользователей за счет размещения информационных ресурсов на территории России.

Горбачев Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна

СРЕДСТВА ЗАЩИТЫ ТЕХНОЛОГИЙ WI-FI И ИХ УЯЗВИМОСТИ

Используемые сегодня технологии Wi-Fi разработаны на основе набора стандартов связи IEEE 802.11, описывающих взаимодействие узлов в беспроводной локальной вычислительной сети (ЛВС). Являясь одной из наиболее популярных технологий связи, представляет собой особый интерес

оценка и анализ их уязвимости с точки зрения обеспечения безопасности и целостности данных при обмене, т.к. наследует все сопутствующие проблемы радиопередачи и протоколов передачи данных. При этом возникает целый ряд вопросов в части достоверной идентификации устройств и аутентификации абонентов сети, используемых методов шифрования траффика, контроля целостности передаваемых данных, а так же возможных векторов атак на сеть.

Изначально (с 1997 г.) стандартом IEEE 802.11 были предусмотрены два метода аутентификации абонента: открытая аутентификация (open authentication) и аутентификация с общим ключом (shared key authentication).

При открытой аутентификации возможен доступ любого абонента к беспроводной ЛВС. Если в беспроводной ЛВС не задействовано шифрование, то любой абонент, знающий идентификатор точки доступа, имеет возможность получить доступ к сети. Однако, в случае использования шифрования, ключи шифрования будут являться средством контроля доступа и если абонент не располагает корректным ключом, то даже в случае успешной аутентификации он не сможет передавать данные через точку доступа и расшифровывать данные, передаваемые точкой доступа.

Аутентификация с общим ключом подразумевает настройку у абонента статического ключа шифрования. Тогда при подключении к сети абонент посылает точке доступа запрос аутентификации, указывая, что нужно использовать режим аутентификации с общим ключом. В ответ точка доступа высылает подтверждение аутентификации, содержащее тестовую строку для шифрования. Если зашифрованная абонентом строка успешно расшифровывается точкой доступа, то абоненту предоставляется доступ к сети.

В качестве алгоритма шифрования в IEEE 802.11a/b/g описывается Wired Equivalent Privacy (WEP), основанный на поточном шифре RC4. К преимуществам данного шифра следует отнести высокую скорость работы, а также возможность использования ключа переменной длинны. Для подсчета контрольных сумм используется алгоритм CRC2. Стандартом предлагается два варианта шифрования: WEP-40 и WEP-104, различающиеся только длинной ключа (40 бит и 104 бит соответственно).

В октябре 2000 г. в опубликованной статье Джесси Уолкера «Unsafe at any key size; An analysis of the WEP encapsulation» были проанализированы недостатки алгоритма, ключевые из которых фактически наследованы от RC4. Проведенное Уолкером исследование получило дальнейшее развитие в двух других работах, опубликованных в 2001 году: «Intercepting Mobile Communications: The Insecurity of 802.11» от сотрудников университета Беркли, и «Weaknesses in the Key Scheduling Algorithm of RC4» (совместно подготовлена специалистами Cisco Systems и факультета вычислительной техники израильского института Weizmann). В этом же году появилась и первая утилита, разработанная Адамом Стаблфилдом, в которой на практике были реализованы теоретические выкладки вышеприведенных авторов, осуществлявшая взлом WEP-шифра за несколько часов.

Так к 2001 г, данный алгоритм оказался уязвимым, а к 2005 г. вовсе потерял свою актуальность. В открытом доступе сегодня все чаще появляются программы, реализующие различные методы атаки на WEP и достигающие результата, менее чем за минуту. Не смотря на отсутствие каких-либо целесообразных причин дальнейшего использования WEP, этот протокол продолжает применяться и сегодня.

В мае 2001 г. группа IEEE Task Group I (TGi) начала работу над новым проектом IEEE 802.11i (MAC Enhancements for Enhanced Security), призванным обеспечить достаточную безопасность в беспроводных сетях. WPA базируется на некоторых компонентах стандарта IEEE 802.11i, принятом в 2004 г., и включает следующие компоненты: протоколы IEEE 802.1x и TKIP (Temporal Key Integrity Protocol).

Стандарт 802.1x использует протокол EAP (Extensible Authentication Protocol), изначально разрабатывавшийся для работы поверх PPP (Point-to-Point Protocol) для передачи сообщений между тремя участниками аутентификации в ЛВС-окружении. Этот вид инкапсуляции известен, как EAP over LANs, или EAPOL. EAP определяет основную структуру для выбора специфического метода аутентификации. При использовании EAP аутентификатору не требуется "понимать" детали различных методов аутентификации. В данном случае он выступает только как промежуточное звено, которое переупаковывает EAP-пакеты при их следовании между саппликантом (supplicant – объект на конце сегмента "точка–точка", которому необходима аутентификация) и сервером аутентификации. Такая технология предоставляет разработчикам возможность выбора между разными видами аутентификации, что следует считать несомненным преимуществом.

Temporal Key Integrity Protocol (TKIP) – второй протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением TKIP использует тот же алгоритм шифрования, что и WEP – RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей: динамические ключи, измененный метод генерации ключей, более надежный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерация пакетов.

В 2008 году на конференции PacSec был представлен способ, позволяющий взломать ключ TKIP, используемый в WPA, за 12–15 минут. Этот метод позволяет прочитать данные, передаваемые от точки доступа клиентской станции, а также передавать поддельную информацию на клиентскую станцию. Однако данные, передаваемые от клиента к маршрутизатору, прочитать не удалось. В 2009 году сотрудниками университета Хиросимы и университета Кобе, Тосихиру Оигаси и Масакату Мории был разработан и успешно реализован на практике новый метод атаки, который позволяет взломать любое WPA соединение без ограничений, причём, в лучшем случае, время взлома составляет 1 минуту.

WPA2 определяется стандартом IEEE 802.11i и призван заменить WPA, в тоже время, являясь его логичным продолжением. В нём реализовано CCMP и шифрование AES, за счёт чего WPA2 стал более защищённым, чем свой предшественник. С 2006 г. поддержка WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

23 июля 2010 года была опубликована информация об уязвимости в протоколе WPA2, обнаруженной сотрудниками компании AirTight Networks, получившей название Hole196. По предоставленной информации, используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ.

Таким образом, анализ уязвимостей технологий Wi-Fi показал необходимость и возможность критического подхода к возможностям используемых технологий, существенно ограничиваемым реальными угрозами информационной безопасности.

Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ИНФОРМАЦИОННАЯ МАСКИРОВКА И ДЕЗИНФОРМАЦИЯ ПРИ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Информация занимает существенное место в развитии науки, техники и экономики как во всем мире, так и в России. А вопросы по защите информационных ресурсов от внешних и внутренних нарушителей не перестают быть актуальными и по сей день. Исследования доказывают необходимость непрерывного развития методов и форм защиты информации и разработки новых современных средств.

Одними из перспективных механизмов, дополняющих существующие механизмы защиты информационных ресурсов, являются механизмы введения в заблуждение(маскирование, дезинформирование, обман) нарушителей. Эти механизмы предназначены для повышения защищенности целевых информационных систем за счет привлечения злоумышленников к ложным информационным целям, введения их в заблуждение, инициирования и идентификации их действий, разоблачения.Обобщенно эти варианты информационного противоборства образуют метод защиты, называемый информационным скрытием. В силу того, что объекты морской инфраструктуры оперируют, как правило, с большими объемами конфиденциальной информацией во всех видах ее представления, необходимость акцентирования внимания на данный метод представляется нам весьма актуальной задачей. Информационное скрытие распространяется на все сферы информационной безопасности, как компьютерной, так и инженерно-технической.

Для выполнения задач защиты компьютерных сетей используются «обманные» системы(ОбС), называемые также ложными информационными системами, имитаторами информационных систем или системами-ловушками. ОбС представляют собой программно-аппаратные средства обеспечения информационной безопасности, реализующие функции сокрытия и камуфляжа защищаемых информационных ресурсов, а также дезинформации нарушителей. В настоящее время существует множество коммерческих и свободно распространяемых ОбС. Они различаются уровнем имитации реальных систем, количеством поддерживаемых протоколов, конструкцией, условиями распространения и т.п. Большинство существующих систем являются уникальными системами, которые имеют возможность имитации определенных сервисов, ОС и приложений, ведут лог (базу данных) действий атакующих и позволяют реализовать различные способы реагирования на атаки.

В вопросе технической защиты информации средства информационного скрытия применялись с самого зарождения технологий радиоэлектронной борьбы(РЭБ) и осуществлялись путем применения имитационных помех. Естественно, вместе с совершенствованием способов создания и применения имитирующих помех развивались и методы помехозащиты, как более или менее эвристические методы обеспечения скрытности, имитостойкости и криптостойкости радиоэлектронных систем и их сигналов.

На определенном этапе развития успехи РЭБ с использованием имитирующих помех способствовали появлению направления активной маскировки излучающих информационных систем от средств радиоэлектронных разведок. А как одним из видов маскировки и основным направлением противодействия техническим средствам разведки выделилась техническая дезинформация.

Опыт использования технической дезинформации и маскировки данных нашел применение также в военной отрасли. Как видом стратегического обеспечения создана стратегическо-оперативная маскировка и дезинформация, организуемая и осуществляемая для решения задач: введения противника в заблуждение относительно состава, состояния и положения маскируемых сил, их возможного оснащения и уровня функциональной готовности; о положении важных стратегических объектов и их защищенности; о планах военного строительства, намерений и решений военно-политического руководства, стратегических планов.

В данном докладе понятия маскировка и дезинформация будут рассмотрены на базе применения их в вышеперечисленных примерах. На опыте использования данных методов показано их особое значение при ведении информационного противоборства с учетом возможностей современных технологий.

Зайнуллин О.Ф.
Россия, Санкт-Петербург, ОАО «СПМБМ «Малахит»

РЕШЕНИЕ ЗАДАЧ НАДВОДНОЙ НЕПОТОПЛЯЕМОСТИ В СИП БЖ ПОДВОДНЫХ ЛОДОК

В более чем полувековой истории отечественного атомного подводного кораблестроения имеется немало славных достижений. Однако были и трагические события, связанные с гибелью кораблей и подводников. задачи надводной непотопляемости для ПЛ были и остаются весьма актуальными. В конце концов, вне зависимости от характера первоначальной аварии, только затопление корабля приводит к его гибели. Поэтому необходимо оснащение кораблей средствами информационной поддержки борьбы за надводную непотопляемость.

Для надводного корабля, как правило, наиболее опасным фактором является потеря поперечной остойчивости. При этом определить запас остойчивости или хотя бы знак начальной поперечной метацентрической высоты простыми методами, например, по параметрам посадки невозможно. Поэтому решение задачи непотопляемости направлено на установление фактического текущего состояния корабля, в первую очередь, установление знака и величины начальной поперечной остойчивости.

Для современной подводной лодки, имеющей форму непроницаемого корпуса, близкую к телу вращения, поперечная остойчивость не является определяющим фактором. Текущие запасы плавучести и продольной остойчивости в первом приближении могут быть определены по параметрам посадки (в первую очередь, по углу дифферента). Если объём затопления не превосходит определённого Спецификацией (как правило, один отсек с двумя смежными, прилегающими ЦГБ),

ПЛ останется на плаву с достаточными параметрами посадки, плавучести и остойчивости при условии прекращения дальнейшего распространения воды. Такие случаи заранее рассчитаны и приведены в корабельной документации, что избавляет личный состав от необходимости выполнения расчётов. До сих пор на кораблях, не оснащённых системами информационной поддержки борьбы за живучесть (СИП БЖ), задача непотопляемости решается вручную. При этом на панелях пультов разворачиваются крупноформатные планшеты, инструкции с различными диаграммами, выполняются расчёты графо-аналитическими методами с последовательными приближениями.

И если в условиях конструкторского бюро для специалиста в области теории корабля поддержки задача занимает около часа, то на борту корабля, в условиях аварии, на качке, когда приходится одновременно руководить борьбой за живучесть, это время значительно увеличивается.

Выполнить же прогноз развития аварии в более или менее реальное время и с необходимой точностью оказывается практически не возможным.На АПЛ 1, 2 поколений и первых лодках 3 поколения реализовать решение задач расчёта надводной непотопляемости в бортовых системах не представлялось возможным в связи с тем, что компьютеры того времени имели значительные массогабаритные характеристики и низкое быстродействие, не позволявшее выполнять расчёты в приемлемое время.

В докладе приведены варианты решения задач надводной непотопляемости в системах информационнойборьбы за живучесть подводных лодок и названы пути преодоления возникающих при этом проблем.

Кальбфляйш В.А., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ ПОЛЬЗОВАНИИ СМАРТФОНАМИ И ПЛАНШЕТАМИ

Обеспечение информационной безопасности (ИБ) пользователей при пользовании техническими средствами массового спроса класса мобильных устройств(МУ) типа смартфонов и планшетов осложнено, как показывает анализ, тем, что собственником техники, как правило, является пользователь (физическое лицо), а не компания (юридическое лицо). Это ограничивает количество

механизмов легального воздействия на него службой ИБ. Вкупе с повсеместным распространением МУ, в том числе и для решения производственных(рабочих) задач, защита смартфонов и планшетов является весьма значимым элементом обеспечения ИБ компаний, предприятий и других юридических лиц.

При этом векторы атак на устройства существенно различаются: от мошеннических приложений, выдающих себя за доверенные (лигитимные), до перехвата интернет-трафика. Причиняемый при этом ущерб от всевозможных атак тяжело переоценить. Так, достаточно только похищенного пароля от ящика корпоративной почты, чтобы получить доступ к конфиденциальной информации компании и, возможно, даже всему электронному документообороту.

Для обеспечения надежной защиты в этом случае требуется применять как стандартный комплекс организационных мер (в том числе по повышению юридически значимой и моральной ответственности и сознательности пользователя), так и ряд программно-технических решений от установки традиционных средств защиты от вредоносных кодов (антивирусов, антиспама и др.) для мобильных платформ до использования систем централизованного управления мобильными устройствами, включая мониторинг уровня защищенности информационных ресурсов компании.

Пользователь, естественно, должен знать о важности установки пароля на доступ к устройству и использовании встроенных в операционную систему(ОС) средств шифрования данных, в том числе и данных на карте памяти. Однако, необходимо повысить его осведомленность овсех потенциальных угрозах и уязвимостях мобильной техники, а также предоставить список обязательных и «крайне рекомендованных» к установке приложений.

Для защищенного подключения к корпоративной сети сегодня, как правило, используют VPN-соединение, а для обеспечения безопасной работы браузера и/или почтового клиента применяют защиту канала связи за счет удаленного сервера (типаSSLVPN).

Контроль обращенияк информационным ресурсам при помощи мобильных решений может быть осуществлен с использованием систем предотвращения утечек информации(DLP-систем), которые способны ограничить доступ к корпоративным файлам только на просмотр и/или предотвратить к ним доступ с мобильных устройств.

Управление многими режимами обеспечения безопасности смартфонов и планшетов может быть выполнено централизовано при помощи систем управления мобильными устройствами (MDM-системы), котораявключает в себя средства шифрования, инструменты для мониторинга и управления устройством, включая удаленное стирание данных, установку и обновление ПО.Средства мониторинга также позволяют отслеживать географическое нахождение устройства и, в случае неадекватной (подозрительной) активности, могут непосредственно задействовать камеру смартфона или планшета.Это порождает новые угрозы, связанные с «вариантностью поведения» пользователей. Получив контроль к данным инструментам, злоумышленник будет иметь возможность осуществлять контроль над всеми устройствами данной сети, включая и данные. Это может привести всю систему ИБ к критическому состоянию. В докладе приводятся и обсуждаются соответствующие практические аспекты технологии защиты.

Более того,остаетсятрадиционная угроза ИБ, обусловленная некомпетентностьюлегитимных пользователейв вопросах должного владения технологиями ИБ. Еще более критичным следует считать в этих условиях инициативное стремление пользователей систематизировать данные обстановки, в том числе в части активного сбора информации о пользователях данной системы без обеспечения должного уровня защиты данных. Понятно, что данные более высокой системной значимости должны иметь более высокий уровень их защиты. Поэтому, тем более, доступ к централизованной системе управления мобильными устройствами должен быть максимально ограничен, защищен, строго и непрерывно контролироваться. Тем не менее, как показывает анализ, этот практически важный вопрос остается проблематичным.

Тем самым, широкий спектр уязвимостей и реальных угроз при пользовании мобильными средствами массового спроса типа смартфонов и планшетов требует специального комплекса мер по обеспечению ИБ.В его основе должен лежать прочный фундамент из «профессиональной сознательности»пользователей (осознанности и самоконтроля ответственности производимых ими действий) и, безусловно, совершенной политики и регламентов безопасности компании.

Карымов А.В., Митько А.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет

ОСОБЕННОСТИ АВТОМАТИЧЕСКОЙ ИНДЕНТИФИКАЦИОННОЙ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДОХОДСТВА

С ростом интенсивности мирового судоходства, появлением высокоэффективных дорогостоящих судов, увеличением их размеров и скоростей повышаются требования к обеспечению безопасности мореплавания. На сегодняшний день в целях повышения безопасности мореплавания во всех морских районах и для повышения эффективности систем управления движением судов (СУДС), разработана современная навигационная система - автоматическая идентификационная

система(АИС). АИС обеспечивает автоматический обмен важными навигационными данными между судами и береговыми станциями в диапазоне ультракоротких волн и значительно дополняет стандартные навигационные комплексы на основе радиолокационных станций (РЛС).

Знание недостатков и ограничений АИС облегчит сложную и объемную задачу по обеспечению безопасности судоходстве. Имея сведения о проблемных сторонах АИС, можно предотвратить множество аварий, к примеру одно из самых разрушительных: столкновение двух судов.

Проблемные зоны АИС условно можно разделить на три типа: недостатки, ограничения, проблемы безопасности в самой системе. Самое значительное ограничение - аппаратура АИС не может заменить другое судовое навигационное оборудование. АИС используется для дополнения средств на основе РЛС. Из ограничений АИС выделяется несколько групп:

1) основные, связанные с насыщенностью судоходства, общим количеством установленного оборудования, достоверностью информацией;

2) ограничения по обнаружение целей, АИС способен обнаруживать судна, только передающие судовую информацию АИС, местность, сбои в работе глобальной спутниковой системе;

3) ограничение по оценке безопасности сближения с обнаруженной целью;

4) ограничение по выбору маневра и оценки ситуации.

Недостатки пересекаются с ограничениями, но больше являются их первопричиной. Большая часть недостатков связана с принципом работы АИС и его установкой, к примеру продуктивное использование АИС, возможно только, если все суда будут оснащены техникой АИС, также АИС никогда не заменит РЛС, который находит объекты отражающие радиоволны, а информация поступающая от неё, числится к объектам с оборудованными транспондерами.

Бреши информационной безопасности в самой АИС, связаны с передачей информации., а именно с радио. Центральная часть АИС - спутниковая система позиционирования, навигационные сенсоры. В каждый определенный промежуток времени АИС отсылает навигационную информацию, причем совершенно открыто. Грубо говоря, АИС - УВЧ радио. Значит АИС можно легко злонамеренно использовать для различных целей, начиная от имитации столкновения, заканчивая отключением АИС транспондеров на других судах.

Несмотря на все проблемные зоны, влияющие на обеспечение безопасность судоходства, АИС остается лучшей современной вспомогательной системой на сегодняшний день. Но знание недостатков данной системы, может легко предупредить аварию. Но не смотря на большое количество недостатков и ограничений АИС, значительная их часть легко перекрывается другими системами, основанными на действии РЛС, что делает АИС довольно устойчивой системой в целом.

В современном мире в судоходстве идет буйный процесс развития и новшеств, но без знания проблемных мест в существующих системах, исправить, а то и направить на пользу, в будущем будет непосильной задачей. А решение предложенных проблем, позволит обеспечить более стабильную информационную обстановку в судоходстве, и повысит уровень безопасности судоходства в целом.

Кузнецов А.Ю., Алексеев А.В.
Россия, Санкт-Петербургский государственный морской технический университет

АВТОМАТИЧЕСКАЯ ДИСТАНЦИОННАЯ МЕДИЦИНСКАЯ ДИАГНОСТИКА И КОНСУЛЬТИРОВАНИЕВ ИНФОРМАЦИОННО ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Вопросы укрепления и сохранения здоровья для человека и общества всегда будут наиболее актуальными. При этом, возможности современной автоматизации медико-диагностических процессов и многих других успешно и непрерывно совершенствуются и, в первую очередь, возможности ранней и объективной диагностики самых различных заболеваний.

Причем, преимущественно – автоматической диагностики, чтобы максимально исключить негативное влияние субъективных качеств медицинских работников, т.е. пресловутого «человеческого фактора» (ЧФ). Как показывает практика, в последнее время именно ЧФ становится одной из наиболее критичных уязвимостей и реальных угроз безопасности пациентов.

Сегодня автоматизированная медицинская диагностика (АрМД)рассматривается, как комплекс математических и технических приемов, осуществляемых с целью повышения достоверности и надежности, ускорения процесса диагностирования. АрМД предполагает частичную или полную передачу функций врача приборам и автоматам, но, непременно, при нейтрализации ЧФ. Одним из наиболее конструктивных путей в этом направлении, по нашему мнению, следует считать переход от АрМД к полномасштабной автоматической диагностике в защищенном исполнении (АтМД-ЗИ), включая дистанционную диагностику и консультирование.

В контексте информационной защищенности пациентов, в том числе от влияния ЧФ, в Российской Федерации принят ряд законодательных актов, обеспечивающей информационную защищенность пациента. Основой в этом контексте являются Федеральные Законы № 152-ФЗ «О персональных данных» и № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Оба закона предъявляют конкретные требования к порядку получения, хранения,

использования, уничтожения информации, содержащей данные о конкретных лицах, о защите персональных данных пациента и предусматривают ответственность за нарушение этого порядка.

Следует учесть, что, если опираться на статью 70 из №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», то АтМД-ЗИ в определенной мере берёт на себя полную передачу диагностических функций врача приборам и автоматам, а за врачом остаются только функции: «утверждения» не вызывающих сомнений принятых АтМД решений; при сомнительных решениях – включение в процесс принятия диагностического решения всего опыта и знаний врача, т.е. «возврата» в режим АрМД и соответствующей ответственности врача.

Традиционно диагностирование состоит из трёх этапов: 1.Сбор информации о больном и проявлениях болезни. 2.Обработка и оценка собранных данных; 3.Принятие решения по диагнозу.

При этом, в целом ряде случаев удается полностью автоматизировать все три этапа (при наличии достоверных алгоритмов диагностирования без участия медицинского персонала).

На 1 этапе формализуется информация о пациенте и явно выраженных симптомах болезни, а также об объективных частных показателях качества здоровья (состояния) пациента (ЧПК по данным клинических, биохимических анализов крови, данным электрокардиограмм, эхограмм, томограмм, рентгенограмм и другим результатам лабораторных исследований).

На 2 этапе систематизируются полученные данные и автоматически рассчитывается комплекс групповых показателей качества здоровья пациента (ГПК) с учетом значимости полученных ЧПК и ГПК (симптомов) для различных заболеваний. Автоматическипо специальным матрицам и алгоритмам этап завершается расчетом агрегированного показателя качества (АПК). По матрице вероятных диапазонов ЧПК, ГПК и АПК автоматически формируется наиболее достоверный вариант диагноза с соответствующей оценкой доверительных интервалов.

На 3 этапе врач анализирует и принимает решение по полученнымрезультатам автоматического диагностирования и состояниюзаболевания в соответствии сознаниями и опытом. В отличии от принятых сегодня в практике в предлагаемом варианте АтМД-ЗИ предусматривается представление результатов анализа и варианта диагноза в текстовом формате и в варианте, близком к интуитивно понятному (доступному и целостному) для пациента.

При этом, необязательно представляется только один вариант диагноза, возможны их альтернативы, что может быть весьма значимым на следующих клинических этапах.

С другой стороны, в случае явного отличия диагноза, устанавливаемого врачом, его аргументация в сравнении с данными АтМД должна быть более убедительной для пациента, чем, например, безапелляционная констатация позиции врача. Это в сочетании с обязательной доступностью для пациента всех (целостных) данных АтМД и обоснования самого диагноза (АтМД или АрМД) обеспечивает более качественное состояние защищенности пациента, в т.ч. от ЧФ.

Более того, такая технология обеспечения информационной защищенности пациента позволяет перейти к дистанционному диагностированию и консультированию при возможности даже самостоятельного ввода данных по результатам полученных пациентом анализов«на руки».

Тем самым, есть основания утверждать, что при масштабной автоматизации процесса диагностирования, как показано в докладе, будут нейтрализованы следующие информационные уязвимости и угрозы пациента:1. Негативное влияние ЧФ в части недобросовестных действий медицинских работников. 2. Ограничение в доступности пациента к данным АтМД и их профессиональной интерпретации. 3.Ограниченные возможности пациента по привлечению независимых экспертов к диагностированию за счет использования, например, каналов дистанционного диагностирования и консультирования. 4. Необоснованные временные затраты. 5. Недостаточная юридическая значимость отдельных медицинских анализов (ЧПК) без их системного анализа, например, в составе рассчитываемых ГПК, АПК и выданного диагноза.

Кроме того, пациент будет более доступным к «неудобным» для врача результатам автоматической диагностики, т.к. врач будет вынужден в этом случае интерпретировать «неудобные» данные автоматических процедур, либо в дальнейшем совершенствовать сам алгоритм принятия решений. Надо признать, что это обстоятельство косвенно «подталкивает»совершенствование самой автоматической медицинской диагностики и её алгоритмов.

Наконец, пациент будет защищён от ошибок поздней диагностики: дополнительная информационная защита пациентов пожилого возраста, как от недобросовестных медицинских работников,«не очень желающих» работать с пациентами пожилого возраста. Последнее будет тем более возможно и малозатратно (по финансам и по времени) при создании и развитии предложенной технологии дистанционного медицинского диагностирования и консультирования.

Рассмотрен пример АтМД-ЗИ при дистанционной диагностике онкологических заболеваний. Для реализации АтМД-ЗИ предложено использовать технологию и программные средства информационной поддержки решений типа «СПРУ» с текстовым, аудио-, фото- и видео-выводом результатов дистанционного диагностирования и консультирования в защищенном исполнении.

КузнецовВ.В., СогоновС.А., АлексеевА.В., ТуркинИ.И., ХруцкийО.В., РавинА.А., ШамберовВ.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской техническийуниверситет

НАУЧНЫЕ НАПРАВЛЕНИЯ И НАУЧНЫЕ ШКОЛЫ ОБЕСПЕЧЕНИЯ РАЗВИТИЯ СИСТЕМ АВТОМАТИЗАЦИИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Разработка перспективных систем судовой автоматики (ССА) объектов морской техники и морской инфраструктуры (ОМТИ) предполагает среди ряда обеспечивающих направлений поступательное и опережающее развитие целого ряда научных направлений, включая, прежде всего:

–развитие теоретических основ автоматизации управления современными сложными эрготехническими системами, включая вопросы теории устойчивости, адаптивных самоорганизующих систем, информационно-аналитической и интеллектуальной поддержки принятия проектных и управленческих решений;

–совершенствование вопросов технологического обеспечения процессов управления судовыми автоматическими и автоматизированными электроэнергетическими комплексами, мониторинга безопасности их эксплуатации с использованием систем комплексной диагностики технического состояния и их логистической поддержки на протяжении жизненного цикла;

–развитие теории и практики системной интеграции и информационно-технического сопряжения разнородных судовых средств обработки и управления информацией в защищенном исполнении, обеспечивающих максимизацию эмерджентных свойств судового оборудования, агрегированных показателей качества ОМТИ и, тем самым, их системную оптимизацию;

Наряду с вопросами технологического совершенствования ССА сегодня в условиях реформирования системы образования в России, включая высшую школу, а также всего комплекса вопросов подготовки и переподготовки кадров, наверное, впервые с особой остротой встает вопрос кардинального повышения качества научного обоснования разработок и их внедрения в нашу отрасль. Судостроение и кораблестроение для России всегда была и останется одной их приоритетных национальных областей развития, но и одновременно - высоко ресурсоемкой и наукоемкой.

В этих условиях традиционным и неисчерпаемым ресурсом обеспечения передовых традиций и достижений в развитии и овладении новой техники и технологий является укрепление научного потенциала отрасли, и, безусловно, научного потенциала высшей школы, системы организации и подготовки кадров. При этом, в первую очередь, в звене развития, поддержки и надежного обеспечения ведущих научных школ отрасли судостроения и кораблестроения.

Сегодня российские специалисты в области корабельной, судовой энергетики и автоматики гордятся именами своих широко известных соотечественников в области развития морской. Созданные ими направления и школы профессионалов высочайшего уровня обеспечили России выход ВМФ в океанскую зону, освоение в мирных целях энергии атома, освоение арктических и антарктических широт, бурное освоения ресурсов океана,

Именно поэтому и с учетом накопленного национального опыта вопрос развития научных школ и соответствующих научных направлений должны стать персональной задачей каждого из руководителей.

В практическом аспекте в интересах развития научных школ, концентрирующих свои задачи в зоне ответственности соответствующих кафедр ведущих университетов и морских академий страны, в том числе кафедры судовой автоматики и измерений СПбГМТУ, к числу перспективных научных направлений, способных перерасти в научные школы с учетом уже накопленного опыта следует отнести и обеспечить поддержку:

–развитию теоретических основ и технологий моделирования сложных организационно-технических систем ОМТИ – руководитель научной школы з.д.н. РФ профессор д.т.н. Розенвассер Н.Г.;

–развитие современных технологий комплексной диагностики и прогнозирования технического состояния морских систем – д.т.н. профессор Хруцкий О.В. совместно с к.т.н.,профессором Равиным А.А.;

–развитие теоретических основ и технологий адаптивных самоорганизующихся систем автоматики критических объектов – д.т.н., профессор Туркин И.И. совместно с к.т.н., доцентом Согоновым С.А.;

–развитие автоматизированных систем интеллектуальной поддержки принятия решений судоводителей в защищенном исполнении, в том числе при мониторинге и управлении борьбой за живучесть критических ОМТИ – д.т.н., профессор Алексеев А.В;

–разработка теории и технологий математического моделирования систем судовой автоматики и оптимизации алгоритмов функционального управления – к.т.н., профессор Шамберов В.Н.

Развитие названных научных направлений в области систем автоматизации объектов морской техники и морской инфраструктуры в сочетании со становлением соответствующих научных школ в

условиях практически неисчерпаемого ресурса талантливых студентов, магистров и аспирантов, высоко квалифицированного профессор-преподавательского состава кафедры во взаимодействии с научными школами других кафедр университетов и академий, научными школами предприятий и организаций отрасли при соответствующем обеспечении комплексом выполняемых научно-исследовательских и опытно-конструкторских работ создаст условия естественного поступательного движения вперед и возможности форсированного освоения новых рубежей научно-технического и технологического развития ССА в комплексе с новым уровнем качества подготовки и переподготовки кадров для судостроительной отрасли.

Кузьменко А.В.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ИНТЕГРИРОВАННЫХ СИСТЕМАХ ПОДДЕРЖКИ БОРЬБЫЗА ЖИВУЧЕСТЬ КОРАБЛЯ

На корабле в аварийной ситуации на счету каждая секунда. Но при этом действует множество взаимных ограничений, связанных с целенаправленной коллективной деятельностью экипажа и технологическими факторами. Командование корабля при боевых и аварийных повреждениях нуждается в точной информации для принятия соответствующих мер по борьбе за живучесть корабля. Фрагментарные противоречивые данные и плохая связь могут еще больше усугубить аварийную ситуацию.

Наличие средств автоматизации на современных кораблях позволяет обслуживать их гораздо меньшими числом членов экипажа, чем это было ранее. Стремление оптимизировать укомплектованность личным составом и функции каждого члена экипажа при этом не должно негативно отражаться на ведении борьбы за живучесть в аварийных ситуациях. Напротив, должно быть компенсировано еще большей поддержкой автоматизированной системы управления. Важно и то, что лицо принимающее решение (ЛПР) имеет возможность не принимать решения, предложенные системой.

Для этих целей были разработаны человеко-машинные интерфейсы, позволяющие операторам осуществлять надзор за действиями системы и взаимодействовать с ней. Известен способ организации человеко-машинного интерфейса, ядром которого является диаграмма опасных состояний и угроз (ДОСУ). Предложенный интерфейс обеспечивает ЛПР обобщенными и детализированными численными прогнозными оценками состояния комплексов боевых и технических средств (БиТС) корабля при воздействии на них поражающих факторов аварии. Интерфейс обладает свойством когнитивности – учитывает психо-физиологические способности человека к восприятию и обработке визуально-динамической информации, а также особенности человека при ориентировании в многомерном изменяющемся пространстве.

Применение человеко-машинного интерфейса имеет существенное значение для работы системы и анализа представляемой информации.

Для более эффективной поддержки принятия решений по управлению борьбой за живучесть в аварийных ситуациях, помимо наличия информации о работе оружия и технических средств и корабельных систем, необходимо прогнозировать развитие аварии, которая, как правило, является комплексной. В такой ситуации выгодно отличалась бы интегрированная система имитационного моделирования аварийных и эксплуатационных процессов, основанная на методах имитационного моделирования и ситуационного анализа, которая включала бы такие компоненты живучести, как непотопляемость, боевая прочность, взрывопожаробезопасность, живучесть оружия и технических средств, защищенность личного состава. Более того, предлагала бы рекомендации по управлению борьбой за живучесть корабля. Следует отметить, что на настоящий момент, как нам известно, не существует разработок, включающих комплекс вышеуказанных элементов, которые были бы программно-алгоритмически взаимосвязаны.

Леберянский А.П.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

ВЗАИМОСВЯЗЬ ЗАДАЧ ПО БОРЬБЕ ЗА ЖИВУЧЕСТЬ И ЗАДАЧ ПО ПРЕДУПРЕЖДЕНИЮ АВАРИЙНОСТИ

В Военно-Морском Флоте сложились три основных направления, по которым ведутся исследования по проблеме живучести кораблей.

Первое направление охватывает вопросы конструктивного обеспечения живучести. Исторический опыт кораблестроения позволил обосновать нормативную базу конструктивного обеспечения живучести и отразить основные требования в документах на проектирование кораблей.

Второе направление решает вопросы развития организационно - технических мероприятий обеспечения живучести кораблей, формирования требований по разработке и совершенствованию

организации обеспечения живучести корабля; внедрения новых методов поддержания средств обеспечения живучести в постоянной готовности к действию.

Третье направление охватывает задачи деятельности личного состава при получении кораблем боевых или эксплуатационных повреждений. Исследования в этой области ведутся методами анализа и обобщения деятельности личного состава корабля при борьбе за живучесть и локализации аварий в реальных условиях боевой подготовки.

Взаимосвязь рассматриваемых вопросов показывает, что живучесть корабля - понятие комплексное, а исследование вопросов живучести имеет свои специфические трудности и ограничения, состоящие в том, что живучесть как свойство корабля в полной мере раскрывается только при получении кораблем повреждений, а до этого она носит скрытый, потенциальный характер.

Однако, использование основных зависимостей теории надежности для оценки живучести корабля в полной мере не представляется возможным, т.к. количественная взаимосвязь живучести и надежности пока не установлена. Некоторые авторы связывают живучесть и надежность как составные элементы более обобщенного понятия - функциональной надежности корабля (судна) в общем "дереве свойств", когда общая функциональность корабля, как сложной системы выступает определенным показателем качества. Для установления количественных показателей качества (к числу которых относят живучесть и надежность) предполагается использовать квалиметрические методы. Однако функциональная взаимосвязь живучести и надежности, малообоснованна, а составленная структурная схема, поясняющая взаимосвязь живучести, надежности и безопасности судна (корабля) выглядит незавершенной.

Понимая такое методологическое несоответствие, делается обоснованная попытка рассмотреть качественное соотношение таких понятий как живучесть, стойкость, надежность и безопасность судна (корабля) как сложной системы в функции от времени Исходной предпосылкой для связи понятий является появление отказа вследствие снижения надежности одной из систем корабля. Следствием отказа, опасного для корабля, является авария, вероятность возникновения которой имеет определенное значение.

В результате возникновения аварии экипаж вынужден выполнять мероприятия по борьбе за живучесть, а после локализации аварии - восстанавливать функционирование систем корабля или всего корабля в целом. Окончательное восстановление эксплуатационных свойств возможно на судоремонтном заводе (аварийный ремонт). Таким образом, представленная графическая интерпретация связи надежности и живучести подтверждает исходную методологическую позицию - живучесть, как свойство корабля, проявляется только после возникновения аварии. Авария возникает под влиянием внутренних (отказ одной из систем корабля), или внешних (столкновение, метеорологические, боевые воздействия) аварийных факторов. Отказ системы является следствием нарушения работоспособности какого-либо элемента.

Отказы системы могут быть постепенными и внезапными. После одних система остается восстанавливаемой, после других - становится невосстанавливаемой. Следовательно, если рассматривать корабль и его экипаж как единую систему, необходимо аналогичную систему понятий ввести для элементов системы (учитывать "человеческий" фактор), но с учетом определенной специфики функционирования экипажа. Однако такого рода методологического единства при рассмотрении соотношений понятий живучести, надежности, стойкости и безопасности как правило не делается. Налицо определенный методологический разрыв в формировании системного подхода к обеспечению живучести. Это приводит к тому, что "участие" личного состава корабля в формировании отказовых ситуаций в теории живучести не рассматривается, чем и обусловлены трудности при формировании структурно-функциональной схемы связи понятий надежности, живучести и безопасности корабля. Существующая методологическая неопределенность может быть снята, если функционирование экипажа до появления аварии рассматривать как комплекс мероприятий, направленных на обеспечение надежности функционирования и предупреждения аварийности, а в случае возникновения аварии (боевого повреждения) - на борьбу за живучесть корабля. Тогда авария выступает тем критериальным показателем, или "граничным условием", которое разделяет процессы функционирования корабля и его технических средств до и после возникновения аварии. До возникновения аварии эти процессы определяются совокупностью всех свойств и качеств его подсистем (боевой готовностью), а действия личного состава представляются управляемыми процессами по обеспечению надежности функционирования и безаварийной эксплуатации, поддержания боевой (технической) готовности в пределах, установленных для заданного оперативного состояния корабля. К этим процессам надлежит отнести мероприятия организационно-технического обеспечения живучести, предупреждения и прогнозирования аварийности.

После возникновения аварии начинает проявляться способность корабля противостоять боевым или эксплуатационным повреждениям, т.е. живучесть, а личный состав корабля осуществляет борьбу за живучесть. локализацию аварии и ликвидацию последствий аварии - восстановление функционирования подсистем корабля, а в целом - в восстановление боевой

(технической) готовности. Следовательно, живучесть - это категория индивидуальной системы первичного уровня (корабля), если рассматривать в целом военно- морской флот как многоуровневую иерархическую систему. На этом принципе решены содержательные и методологические основы боевой подготовки личного состава по борьбе за живучесть, разработаны определенные количественные нормативы и показатели для оценки качества и уровня живучести корабля в целом.

Однако, правильно трактуя конечные результаты, формы и методы организации борьбы за живучесть, научные принципы живучести корабля не могут раскрыть системную сущность предупреждения аварийности, единства всей многоцелевой работы, проводимой в ВМФ по снижению аварийности. Налицо складывается видимое противоречие, проявляющееся в условиях повседневной эксплуатации кораблей (при отсутствии боевых повреждений) - когда уровень подготовки по борьбе за живучесть отвечает требованиям руководящих документов по боевой подготовке, а число аварий и аварийных происшествий (технических и навигационных), остается достаточно высоким.

Выполненный достаточно подробно анализ причин, приводивших к авариям и аварийным происшествиям, показал, что основная доля причин приходится на так называемый "человеческий" фактор, который в свою очередь можно разбить на четыре группы: социальные, профессиональные, психологические и организационные. И только 17% составляют категорию причин, которые можно определить, как технические.

Самая многочисленная группа причин, составляющая 54,5% является социальной, а которую включены такие причины, как нарушение требований руководящих документов личным составом кораблей, низкая организация службы на корабле и ГКП, безответственность, не-дисциплинированность, отсутствие контроля со стороны должностных лиц и др.

Низкая профессиональная подготовка личного состава является причиной 28,9% аварий и аварийных происшествий. Появление такого противоречия в общеметодологическом плане можно рассматривать как результат функционирования некоторой сложной эргатической системы (экипажа корабля), на выходе которой имеет место один из ее показателей - уровень подготовки личного состава к борьбе за живучесть, а на входе - целая группа факторов аварийности, в числе которых основную долю составляют факторы некачественного функционирования эргатических элементов этой же системы.

Таким образом, достигнутый уровень боевой подготовки (ресурс экипажа) растрачивается на локализацию аварий или аварийных происшествий в ходе борьбы за живучесть. Следовательно возникает двуединая задача - в ходе планирования и организации боевой подготовил обеспечить максимальный ресурсный уровень экипажа (внутренняя задача), и уменьшить "весовую" значимость группы человеческих факторов аварийности (внешняя задача). И если решение внутренней задачи достигается существующим многообразием форм и методов боевой подготовки, разработанной документацией и системой подготовки и контроля готовности экипажа к борьбе за живучесть, то решение внешней задачи в практической деятельности ВМФ осуществляется без должной эффективности. Это, в первую очередь, объясняется отсутствием теоретических основ предупреждения аварийности, методологической неопределенностью категорий предупреждения аварийности, двойной природой диалектического единства и противоположности предметной и операциональных сторон понятий "живучесть корабля" и "предупреждение аварийности".

В Военно-Морском флоте понятие "живучесть корабля" имеет достаточно определенную трактовку, закрепленную Корабельным уставом ВМФ и включенную в Руководство по борьбе за живучесть корабля:

Живучесть -"... способность корабля противостоять боевым и аварийным повреждениям, восстанавливая и поддерживая при этом в возможной степени свою боеспособность".

Однако, несмотря на однозначность определения «живучесть корабля» принятого в ВМФ в соответствии с действующими руководящими документами и ГОСТ, судостроительная наука продолжает исследования по вопросам формирования связей понятийного аппарата живучести суд-на, надежности судна, безопасности судна.

Исторический процесс совершенствования мер по обеспечению живучести корабля и подготовки личного состава по борьбе за живучесть и локализации аварий имеет глубокие корни и тесно связан с развитием кораблестроения. Этот опыт показывает, что там, где мы старые, на первый взгляд понятия, старое содержание формулируем по-новому, в рамках новой, более широкой теории, мы всегда получаем нечто большее, чем просто новое повторение старого. Само "старое" получает в рамках новой понятийной системы новое содержание. Интерпретация "старого", но уже в новой системе часто является началом новых проблем.

В этой связи представляется, что проблема предупреждения аварийности, которая сама по себе - чрезвычайно сложное и многофакторное явление, требует для своего решения системного подхода к объектам исследования, так как в ходе длительной практической деятельности флота выработаны и документально закреплены определенные организационно-технические и организационные мероприятия, направленные на обеспечение живучести и предупреждение аварийности. Тогда, предупреждение аварийности, возможно трактовать как систему организационно-

технических мероприятий и методов боевой подготовки по исключению навигационных и технических происшествий с кораблями (судами) ВМФ и обеспечению требуемого уровня их боевой готовности.

Структура составляющих трактовки "предупреждения аварийности", позволяет заключить, что «предупреждение аварийности» является категорией всех флотских уровней, а "безаварийность", как интегральный показатель эффективности системы мер, отражает качественное свойство такой системы.

Отсутствие реальных возможностей измерения и оценки качества предупреждения аварийности прямым, опытным путем в «натурных» условиях, выдвигает на первое место необходимость разработки различных методов научного анализа и синтеза мер по предупреждению аварийности на базе единых методологических и теоретических принципов.

Важным практическим результатом такого подхода является возможность снятия методологической неопределенности при решении практических задач по снижению аварийности в военно-морском флоте, возникшей в результате отсутствия теоретических основ предупреждения аварийности. Диалектическим базисом любой теории является практика. "Жизнеспособны лишь те научные направления, которые идут от практики и возвращаются к ней»

Поэтому изучение и анализ опыта по решению задач предупреждения аварийности и обеспечения живучести в различные периоды деятельности флота в мирных и боевых условиях составляют важный элемент логической последовательности военно-научного познания.

Лобанов С.Л., Бледнов Д.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

ЭВОЛЮЦИЯ ТРЕБОВАНИЙ К АВТОМАТИЗАЦИИ ПРОЦЕССА БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ,СУДНА

Автоматизация действий по борьбе за живучесть (БЖ) экипажей кораблей (судов) является одним из тех направлений в развитии военного кораблестроения, которые связаны со снижением уровней возможных ущербов корабля (судна) при возникновении аварии. Цель автоматизации – в повышении эффективности противоаварийных действий личного состава путем оптимизации плана этих действий, сокращении времени их выполнения, исключении человеческих ошибок.

За последние несколько десятков лет требования к процессу автоматизации действий по БЖ кораблей (судов), которые реализовываются в соответствующих системах управления (СУ), значительно изменились. Для более объективного рассмотрения эволюции этих требований последние целесообразно рассматривать применительно к трем различным группам личного состава кораблей и судов, участвующим в борьбе с возникшим пожаром:

– руководящий состав, принимающий решения по борьбе с пожарами;

–личный состав среднего звена, реализующий принятые решения дистанционно, с пультов управления;

–личный состав отсеков, помещений корабля (судна) и аварийных партий, реализующий принятые решения вручную.

Принятое деление действий экипажа по БЖ в значительной степени носит условный характер, однако в конечном счете позволяет более четко и последовательно вскрыть основные проблемы автоматизации БЖ и пути их решения, структура которых представлена в следующей таблице.

Известно, что деятельность руководящего состава корабля, прежде всего командира корабля (КК) и командира БЧ-5 (КБЧ-5) при БЖ является одним из наиболее сложных в психологическом и информационном отношениях видов человеческой деятельности. Рассматривая многочисленные аварии на отечественных и зарубежных кораблях и судах, можно привести многочисленные примеры ошибочных и запоздалых решений этой категории лиц по управлению аварийным кораблем, охваченным пожаром, и его техническими средствами (ТС), приводивших к усугублению аварий, а, порою, и к катастрофе корабля. Неслучайно поэтому в начале 60-х годов перед соответствующими организациями ВМФ и промышленности была поставлена задача создания для кораблей автоматизированной системы борьбы за живучесть (АСУ БЖ), прежде всего в части борьбы с пожарами. При этом под автоматизацией действий человека понималось его полное исключение из контура управления в решении тех или иных задач борьбы с пожаром путем замены его автоматизированной системой (подсистемой) управления. Однако, несмотря на особую значимость, поставленная задача решена не была.

Причины такого положения дел лежали в особо сложном, трудно формализуемом характере деятельности руководящего состава корабля при борьбе с возникшим пожаром. Поэтому требования к автоматизации процесса управления кораблем и его ТС при борьбе с пожарами были эволюционизированы, т.е.существенно изменены. Наиболее реальным путем повышения эффективности деятельности руководящего состава кораблей (судов) как при борьбе с пожарами, так и в целом при БЖ в настоящее время признано оказание для него информационной поддержки в процессе принятия ими тех или иных решений по руководству БЖ на корабле. Поэтому задач,

связанных с полной автоматизацией процесса принятия решений при БЖ и их реализацией, для рассматриваемой группы лиц, в настоящее время не ставится.

Требования к автоматизации процесса БЖ кораблей (судов) ВМФ за последнее десятилетие значительно изменились и стали значительно более жесткими, прежде всего к проектантам СУ. Однако ряд проблем автоматизации этого процесса остался не решенным до настоящего времени. Пути их решения - разнообразны и зависят от того уровня иерархии в процессе БЖ, который занимает лицо, вовлеченное в этот процесс. Данные пути могут носить организационный характер и связаны с оснащением кораблей (судов) уже созданными к настоящему времени системами информационной поддержки БЖ. Но могут содержать в себе необходимость выполнения научных исследований, проработок и ОКР, например, в части перевода слухо-речевой информации, возникающей в ходе БЖ, в визуальную. Однако независимо от направленности реализация этих путей должна привести в конечном итоге к повышению эффективности процесса БЖ и снижению возможных ущербов при возникновении аварий на кораблях (судах) ВМФ.

В докладе выполнен анализ эволюции требований к автоматизации процесса борьбы за живучесть кораблей (судов) ВМФ. Вскрыты существующие в настоящее время проблемы автоматизации борьбы за живучесть применительно к различным категориям личного состава, предложены пути их решения.

Малов С.С., Шиманчук С.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕДАЧИ ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ КРЮИНГОВОЙ ОРГАНИЗАЦИИ

При построении комплексной защиты информационной системы персональных данных далее (ИСПДн) администраторам информационной безопасности крюинговой компании приходится реализовывать механизмы защиты направленные на защиту персональных данных (далее ПДн), обрабатываемых в пределах контролируемой зоны организации, а так же при передачи этих данных за пределы контролируемой зоны с использованием сети общего пользования Интернет, с учетом того, что передача может осуществляться, как в пределах одного государства, так и за его пределы. При этом необходимо обеспечить безопасности защищаемой ИСПДн от внешних угроз, а также безопасность передаваемых ПДн при их нахождении за пределами контролируемой зоны.

ИСПДн крюинговых компаний, в которых обрабатываются специальные категории персональных данных менее 100 тысяч субъектов персональных данных при условии, что ИСПДн актуальны угрозы 2-го типа, необходимо обеспечить 2 уровень защищенности. Данные требования вытекают из требований Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Далее, после определений уровня защищенности, необходимо определить перечень технических мер направленных на защиту передаваемых данных. Для этого необходимо использовать положения приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн».

Согласно положениям вышеуказанного приказа для организации защиты внешнего периметра ИСПДн, соответствующего 2-му уровню защищенности, необходимо использование межсетевых экранов не ниже 3 класса защищенности. Использование межсетевых экранов, которые соответствуют необходимому классу защищенности, позволяет говорить о выполнении нормативных требований в данной части.

В процессе самой передачи, когда данные находятся за пределами контролируемой зоны обеспечить их безопасность возможно двумя способами:

1. Передача данных с использованием технологии Virtual PrivateNetwork (далее VPN).
2. Организация шифрования данных перед их передачей за пределы контролируемой зоны и соответствующей расшифровкой их по получению адресатом.

VPN – это технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети, например сети Интернет. Таким образом, с помощью VPN можно создать защищённое удалённое подключение между филиалами компании и главным офисом, а также между компаниями, находящимися в разных странах. VPN имеет ряд преимуществ: для работы VPN-сессии нужен только браузер, доступ настраивается быстро, высокая безопасность и аутентификация данных, перебои связи не вызывают обрыва VPN-соединения. Из недостатков можно отметить, что для использования подобной технологии необходимо иметь периоды смены шифровальных ключей, чтобы сохранять безопасность ПДн на высоком уровне.

Шифрование же представляет собой изменение читаемой информации в нечитаемую. Видимый хаотичный результат, однако, подчиняемый определённым правилам и алгоритмам,

который позволяет с помощью подходящего шифра или ключа расшифровать ценную информацию. На данный момент широко представлены системы, как с симметричным, так и с асимметричным шифрованием. Но шифрование тоже не безупречно. Недостатком симметричного шифрования является необходимость публичной передачи ключей, что делает невозможным использование данного вида шифрования с неограниченным количеством участников. У асимметричного же шифрования низкая скорость выполнения операций расшифровки и зашифровки, что обусловлено необходимостью обработки ресурсоёмких операций.

Какой способ выбрать для обеспечения защищённой передачи ПДн решается непосредственно руководителем крюинговой компании с использованием риск ориентированного подхода на основании ранее полученных в процессе обследования ИСПДн данных.

Мельников А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

В России с 1 января 2008 года вступила в силу «Права на результаты интеллектуальной деятельности и средства индивидуализации» (4 часть Гражданского Кодекса, Федеральный закон от 18.12.2006 № 231-ФЗ, раздел VII). Они определяют интеллектуальную собственность, как список результатов интеллектуальной деятельности и средств индивидуализации, которым предоставляется правовая охрана.

В положении Конвенции ООН об учреждении Всемирной организации интеллектуальной собственности, членом которой является Россия, записано: интеллектуальная собственность включает права, относящиеся к литературным, художественным и научным произведениям, исполнительской деятельности артистов, звукозаписи, радио- и телевизионным передачам, изобретениям во всех областях человеческой деятельности, научным открытиям, промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям, относящимся к защите против недобросовестной конкуренции, атакже все другие права, имеющие отношение к интеллектуальной деятельности в производственной, научной, литературной и художественной областях.

Однако, в настоящее время практически нет защиты против недобросовестной конкуренции. Практика показывает, что недостаточно осуществляется и охрана авторских прав на изобретения, научные открытия. Очень серьезна проблема ведомственной разобщенности в сфере интеллектуальной собственности и ее охраны. Известно, что здесь традиционно разделены сферы авторского права: Бернская, Женевская конвенции защищают произведения науки, литературы и искусства и патентного права; Парижская конвенция — промышленную собственность: изобретения, открытия, промышленные образцы, рационализаторские предложения и т.п. Делаются попытки провести между этими сферами четкие границы. Так, считается, что авторское право ориентируется на форму, а патентное — на содержание творческого результата.

Однако, как известно, форма часто сливается с содержанием. Например, патентное ведомство Великобритании на издаваемых им патентных описаниях ставит копирайт, т.е. знак защиты авторского права. Существуют и технические объекты, где форма и содержание неделимы.Другим основанием для разграничения может считаться сам способ построения вышеупомянутых сфер права. Авторское право строится, как защита реноме автора, творческого результата, который является объективно неповторимым.

Патентное право строится, как защита приоритета, творческого результата, который может появиться одновременно у разных авторов. Поэтому авторство нужно вовремя регистрировать, подавать заявку, фиксировать приоритет, проводить экспертизу на новизну.

Практика показывает, что недостаточно совершенны механизмы согласования, основанные не на указаниях, а на следовании общим экономическим интересам. Следует стремиться к тому, чтобы «помочь готовить специалистов в таких областях, как управление исследованиями, научная и техническая политика, экспертиза конкурсных заявок, сертификация, управление высшим образованием, передача технологий, маркетинг научно-технической продукции, защита интеллектуальной собственности».

Закон «Об авторском и смежных правах» (статья 48-1) содержит требование принятия технических мер защиты авторского права и смежных прав. Однако, до сих нет никакой ответственности за невыполнение этих требований. Поэтому необходимо регламентировать эти изменения. Указанные статьи отвечают передовым тенденциям в развитии международного права в сфере авторского права, в частности ст. 11 Договора ВОИС по авторскому праву, в которой говорится о соответствующей правовой охране и эффективных средствах правовой защиты существенных технических средств, используемых авторами в связи с осуществлением их прав.

Кроме того, указанные требования согласуются с Директивой ЕС 2001/29/ЕС от 22 мая 2001г. "О гармонизации определенных аспектов авторских и смежных прав в информационном сообществе". Тем не менее, данная Директива делает существенный шаг дальше, чем корреспондирующие положения Договора ВОИС. В соответствии с Директивой запрещается не только обход таких технических мер защиты, но и производство или продажа оборудования, предназначенного для такого обхода. В этом же направлении развивается российское законодательство в Законе об авторском праве (ст. 48-1).

Под техническими средствами защиты авторского права и смежных прав согласно п. 1 ст. 48.1 Закона понимаются любые технические устройства или их компоненты, контролирующие доступ к произведениям или объектам смежных прав, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором, обладателем смежных прав или иным обладателем исключительных прав, в отношении произведений или объектов смежных прав.

В п. 2 ст. 48.1 Закона конкретно сформулирован запрет на обход технических средств защиты авторских и смежных прав.Однако, анализ упомянутых выше положений, в целом эффективных для защиты интересов правообладателей, приводит к неутешительному выводу о том, что они пока представляют собой «холостой выстрел» в направлении потенциальных правонарушителей. Во-первых, эти положения не подкреплены ссылками на соответствующие санкции за их нарушение.Во-вторых, такие санкции, равно как и составы правонарушения, согласно особенностям, российского права должны быть сосредоточены в КоАП РФ и в УК РФ.

Таким образом, защита интеллектуальной собственности в области информатики, компьютерной техники, наукоемких высоких технологий не случайно выдвигается на передний план. Это связано с усложнением как стратегического, так и тактического управления, которое сегодня все в большей мере становится важнейшим ресурсом, определяющим прогресс общества.

Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СИСТЕМА УПРАВЛЕНИЯ ДВИЖЕНИЕМ СУДНА ПО КУРСУ С ПОВЫШЕННОЙ ЖИВУЧЕСТЬЮ

От их качества и надежности системы автоматического управления движением судна по курсу – авторулевого (АР) в значительной степени зависит безопасность мореплавания, а также технико-экономические показатели эффективности эксплуатации судов. Судно, как объект системы автоматического управления движением по курсу, является сложным гидродинамическим звеном, состоящим из корпуса судна, руля и окружающей их среды. Точное математическое описание такого звена встречает большие трудности, а получаемые при этом нелинейные уравнения чрезвычайно сложны. При этом гидродинамические коэффициенты уравнений значительно изменяются с изменением скорости хода судна и его загрузки, т.е. судно является нелинейным нестационарным объектом.

Традиционным законом управления в авторулевых является ПИД-закон. Однако, уже в начале 70-х годов начались интенсивные работы по созданию новых, более эффективных систем автоматического управления движением судна. Одним из основных направлений решения этой проблемы являлось создание автономных адаптивных авторулевых, обеспечивающих в большинстве случаев автоматическую настройку параметров (параметрическую адаптацию) системы при изменении состояния объекта управления и внешних условий плавания (скорости хода, осадки судна, состояния погоды, глубины под килем).

Опыт эксплуатации таких адаптивных авторулевых подтвердил повышение их технико-экономической эффективности по сравнению с традиционными авторулевыми.При стабилизации курса морских среднетоннажных и крупнотоннажных судов в АР используется параметрическая адаптация. Такие АР относятся к самонастраивающимся системам. В общем случае при оценке качества управления курсом учитывается только точность поддержания задаваемого курса, величина и рациональность перекладок руля.

В адаптивных АР применяют обычно два варианта критерия качества- экономический и безопасности. В самонастраивающихся АР условно можно выделить системы с пассивной, активной и комбинированной адаптацией. Пассивная адаптация применяется, когда факторы, влияющие на качество регулирования, измеряемы, их можно рассчитать, как изменить параметры АР, чтобы качество управления осталось хорошим. При такой адаптации коэффициенты закона регулирования находятся по определенной программе в зависимости от результатов контроля возмущений.

Самонастраивающиеся системы с активной адаптацией делятся на поисковые, аналитические, аналитически-поисковые. Активная адаптация более сложна, требует времени на поиск значений коэффициентов регулятора или на оценку параметров модели объекта по оперативной информации. Однако она по сравнению с пассивной адаптацией имеет более широкий диапазон применения и замкнутый контур самонастройки, обеспечивающий достижение действительного экстремума

функции качества. Поэтому в адаптивных АР чаще всего применяется комбинированный способ адаптации, позволяющий в той или иной мере наилучшим образом использовать достоинства как активной, так и пассивной адаптации.

Авторулевые с элементами искусственного интеллекта создаются на основе методов нечеткой логики и нейронного управления.Достоинством обоих видов систем является ненужность для получения решения задачи точного описания динамики объекта управления. Но отсюда следует и их общий недостаток - невозможность аналитического исследования качества.

В заключение краткого анализа можно отметить, что каждый метод параметрической адаптации обладает своими недостатками и достоинствами. Однако, применение таких авторулевых позволяют только частично решить проблему адаптивного управления судном как нелинейным нестационарным объектом в категориях теории управления, так как потенциальные возможности параметрической адаптации ограничены, и при этом совершенно не решается проблема их живучести.

Настало, вероятно, время изменения этого положения с появлением перспективного класса адаптивных систем – самоорганизующихся с высоким уровнем искусственного интеллекта, которые могут одновременно реализовывать структурную (функциональную) адаптацию с алгоритмами параметрической адаптации.

Принципиальное отличие этих систем управления от известных адаптивных систем состоит в том, что они построены на сочетании алгоритмов структурной (функциональной) адаптации с алгоритмами параметрической адаптации и оптимальностью.

Для определения особенностей оптимального самоорганизующегося авторулевого с повышенной живучестью и традиционного авторулевого с ПИД-законом было выполнено имитационное моделирование их работы применительно к судну с водоизмещением 6000 т. Сравнительный анализ систем позволил сделать вывод: повышение живучести, надежности и безопасности авторулевых может осуществляться на основе адаптивных систем с высоким уровнем искусственного интеллекта.

Москаленко В.А., Калюта Н.Г.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

МОДЕЛЬ ЖИВУЧЕСТИ КОРАБЛЯ И ЕГО ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ ВНЕШНИХ ПОРАЖАЮЩИХ ВОЗДЕЙСТВИЯХ

Современные корабли представляют собой сложные технические системы высокой степени иерархии. В них собраны в единый комплекс разнообразное оружие и технические средства с различным характером боевого и повседневного функционирования, а также степенью влияния на эффективность выполнения поставленных задач. В отличие от других боевых систем (танки, самолеты и т. д.) корабли являются самыми дорогими и малосерийными системами.

Для анализа корабля, в качестве сложной системы необходимо определить систему как множество компонентов, взаимодействующих друг с другом и служащих общему назначению, или цели.

В докладе рассматривается живучесть, как функциональное свойство сложной системы – корабля и его технических средств. Живучесть судна, как известно, есть способность противостоять воздействию стихийных сил ветра и волн, пожаров, оружия противника, а при повреждениях сохранять и восстанавливать полностью или частично мореходность и боевые качества.

Все факторы, определяющие живучесть систем, предложено разделить на три группы по функциональному признаку: факторы, характеризующие внешние поражающие воздействия;факторы, характеризующие собственные свойства системы и отдельных ее элементов с точки зрения живучести; факторы, обеспечивающие взаимодействие с внешними системами борьбы за живучесть, а именно наличие оперативных и надежных средств связи системы с внешними средствами, возможность своевременного и эффективного вмешательства внешних средств (сил) в борьбу за живучесть корабля.

Предложены показатели, которые позволяют дать только общую интегральную оценку живучести кораблей. Для оценки качества проектных решений в части живучести технических систем в процессе получения боевых повреждений необходимо проанализировать живучесть его технических средств при получении поражающих воздействий с учетом накопления ущерба с целью его минимизации и обеспечения возможности выполнения кораблем поставленной задачи. Таким образом, задачей моделирования живучести корабля является структурно - функциональная оптимизация технических средств корабля с учетом возможностей конструктивной защиты.

Модель живучести корабля, как сложной системы представляет собой совокупность большого числа частных моделей различного назначения, использующих для описания процессов как детерминированные, так и вероятностные методы.

Исследование структурной составляющей живучести в основном сводится к выявлению уязвимых мест в топологии системы и определению степени их влияния на целостность системы. Исследование функциональной составляющей живучести сводится к определению способности системы решать стоящие перед ней задачи при изменяющихся возможностях ее элементов.

Непредсказуемость изменения большинства факторов, влияющих на свойства систем и их топологию, придает особое значение оценке функциональной составляющей живучести с учетом состояния элементов системы и действующих между ними взаимосвязей.

Техническая система представляет собой распределенную структуру, размещенную по всему кораблю. Схема функционирования её задается с помощью графа, который определяет физическую структуру системы, его ребра, соответствуют физическим компонентам (трубопроводы, кабельные трассы и т. д.), приложенным от одной вершины графа (насоса, электродвигателя, щита и т. д.) к другому.

При получении поражающих воздействий с эпицентром в определенных координатах определяются пораженные помещения (отсеки) корабля.

При многократных поражающих воздействиях процесс циклически повторяется с получением набора работоспособных и неработоспособных структур систем, оценки живучести систем и корабля в целом до достижения ее критического значения

При моделировании могут инициироваться процессы возникновения пожаров и затопления отсеков корабля как следствие поражающих воздействий. В результате поражающих факторов вторичных аварийных процессов происходит поражение элементов технических систем в результате затопления отсеков, пожаров и других факторов.

Пегушин О.В., Аскеров Р.А., Москаленко В.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ РИСКОВ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ РАБОТ ПО ВОССТАНОВЛЕНИЮ ТЕХНИЧЕСКОЙ ГОТОВНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЕЙ ВМФ РФ

Случаи аварий и катастроф, гибели и травматизма личного состава на кораблях ВМФ специалисты в области военного кораблестроения связывают прежде всего с недостаточным обеспечением их безопасности. Об этом свидетельствуют материалы в средствах массовой информации об авариях кораблей, руководящие и эксплуатационные документы, регламентирующие методы и тактику борьбы с возникшей аварией на кораблях ВМФ, а также ряд совместных решений командования ВМФ и промышленности по конструктивному и организационно-техническому обеспечению живучести проектируемых заказов.

При аварийных повреждениях корабль, как правило, находится вне боя и непосредственное решение каких-либо боевых задач, ради чего он и создавался, т.е. функционирование корабля по прямому назначению, отходит на второй план. Главным свойством корабля, которое необходимо обеспечить в ходе противоаварийных действий, становится не живучесть, а безопасность.

Свойство «безопасность» в действующем государственном стандарте о свойствах и характеристиках современных кораблей определяется «как способность корабля сохранить при выполнении поставленных задач в конкретных условиях в течение установленного времени состояние, при котором исключено или снижено до допустимых значений воздействие опасных или вредных факторов на личный состав, а также окружающую природную среду и местное гражданское население».

При рассмотрении аспектов безопасности принят постулат, что абсолютной безопасности не существует − после принятия защитных мер некоторый остаточный риск всегда остается.

Безопасность достигается путем уменьшения риска до допустимого уровня, определенного как допустимый риск. Допустимый риск есть результат поиска оптимального баланса между идеалом абсолютной безопасности и требованиями, которым должны удовлетворять корабли, их эксплуатация, а также такими факторами, как выгодность для использования, соответствие цели, эффективность затрат.

Это означает, что существует необходимость постоянного пересмотра допустимого уровня риска, в особенности, когда развитие технологий и знаний может привести к экономически оправданным усовершенствованиям, чтобы достичь минимума риска, связанного с использованием кораблей.

Допустимый риск достигается с помощью итеративного процесса общей оценки риска (анализа риска и оценивания риска) и уменьшения риска.

Для уменьшения рисков до допустимого уровня рекомендуется использовать следующую процедуру:

– определить возможные группы обслуживающего персонала технических средств при боевом использовании или техническом обслуживании (включая группы офицеров и старшин) и уровень

подготовки (например, при сдаче задач кораблем, ремонте, сроков службы личного состава, а также возраст);

– определить предназначенное использование и выявить возможное предсказуемое неправильное использование корабля при боевом использовании или техническом обслуживании;

–выявить каждую опасность (включающую любую опасную ситуацию и вызывающее ущерб событие), возникающую на всех этапах и при всех условиях использования корабля, его боевого применения или отработки задач, включая постройку, эксплуатацию, ремонт, утилизацию;

– оценить риск для каждой определенной группы специалистов (офицеров и старшин) или обслуживающего персонала предприятий, возникающий вследствие определенных опасностей;

– принять решение, является ли риск допустимым при эксплуатации технических средств на данном этапе жизненного цикла корабля;

– если риск является недопустимым, уменьшить его до допустимого значения.

Пиглюк Р.Н., Шавинская С.К.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

РАЗРАБОТКА МЕТОДА СРАВНЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ЗНАНИЙ

В настоящее время все больше коммерческих сделок, деловых операций и государственных функций осуществляется через Internet, в частности через World Wide Web. Многие из этих операций должны быть секретными. К ним относятся покупки, выписывание счетов, банковские услуги, правительственные распоряжения и т.п. Как правило, для этих приложений необходимы аутентификация, секретность и невозможность отрицания авторства. Эти возможности могут обеспечить простые криптографические протоколы, такие как TLS (или SSL). (TLS (англ. Transport Layer Security - безопасность транспортного уровня), как и его предшественник SSL (англ. Secure Sockets Layer - уровень защищённых сокетов) - криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Internet. Данные протоколы широко используется в приложениях, работающих с сетью Internet, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями.)

Однако существует множество операций, которые также можно выполнить с помощью Internet, но невозможно защитить простыми протоколами вроде TLS.К таким операциям относятся микроплатежи (необходимо максимально удешевить транзакции), электронные платежи (необходимо сохранить анонимность и предотвратить вымогательство), аукционы (необходимо отделить выигравший лот от проигравших), голосование (необходимо сохранить анонимность голосующих и предотвратить принуждение), обмен (необходимо соблюдать справедливость, учитывая, что участники обладают разными ресурсами), временные метки и подтверждение подлинности (необходимо заверить подлинность сообщения), восстановление синхронизированных ключей.

Более тонкие операции требуют более сильных криптографических протоколов. Одними из таковых являются протоколы с нулевым разглашением (нулевой передачей знаний). Протоколы с нулевым разглашением представляют собой активно разрабатываемую область криптографии, связанную с компьютерными науками. Доказательства с нулевым разглашением находят важные практические сферы применения, например, в области разработки протоколов для интеллектуальных карточек. Поэтому на первом этапе одной из самых актуальных задач является исследование различных протоколов с нулевым разглашением по различным критериям. В качестве критериев могут быть выбраны: коммуникационные затраты, вычислительные затраты, гарантии безопасности, необходимость наличия доверенного центра.

Необходимо рассмотреть основные схемы с нулевой передачей знаний, выявить и обосновать выбор основных параметров для сравнения протоколов и произвести сравнительный анализ представленных протоколов по основным критериям, а также разработать метод сравнения криптографических протоколов с нулевым разглашением по вышеперечисленным параметрам.

Основной целью предлагаемой Методики комплексной оценки рисков и обеспечения безопасности при проведении работ по восстановлению технической готовности ТС кораблей ВМФ является выработка понятного и применимого на практике алгоритма выполнения аварийных ремонтно-восстановительных работ, с целью введения в строй технического средства и обеспечения при этом безопасности личного состава, недопущению его гибели и травматизма.

Практическое применение методики рассмотрено на примере проведения ремонтно-восстановительных работ по замене насос - форсунки на дизель - генераторе типа 30ДГ. Содержание работ – снятие с дизеля, разборка, проверка распылителя, сборка и испытание, установка на дизель насос – форсунки в соответствии с технологической картой Инструкции по техническому обслуживанию дизель – генератора 30ДГ.2ИО.

Поленин В.И., Можаев А.С., Можаева И.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

КОНЦЕПЦИЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ МАКРОУРОВНЕВОГО ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ВЫПОЛНЕНИЕМ ЗАДАЧ С ПРИМЕНЕНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ

Организация функционирования системы управления выполнением целевыхзадач на основе сетевого планирования определяется многообразием, множеством агентови сложностью структурных взаимосвязеймежду ними, недоступностью для мониторинга руководителем процесса выполнения задач (ЛПР).

Все операционные модели объединяет важное существенное свойство: ониактивны в действиях или в состояниях. Глобальное поведение системы возникает как результат действийили изменения состояний многих операций, каждая из которых взаимодействует со средой и с другими операциями. В управляемой системе операции осуществляются по единой политике, определяемой замыслом выполнения целевой задачи и проводимой с помощью командно-сигнального управления.

Управляемоеосуществление операцийможно отождествить с наступлением соответствующих событий. События – второй общепринятый термин для широкого класса логических и вероятностных моделей.

Система организационного управления выполнением задач, сформированная из операций и сопутствующих им событий, есть необходимое и достаточное средство поддержки высшего уровня управленческой деятельности командного состава кораблей и судов. Для радикального отличия этой системы от всех известных традиционных систем организационно-технического управления целесообразно придать ее названию атрибут «макроуровневого», который характеризует свойственный ей уровень организационного управления: «Система автоматизированной поддержки макроуровневого организационного управления выполнением задач».Поддержка состоит в доступном для восприятия ЛПР мониторинге процесса выполнения задачи, обычно воспроизводимого лишь мысленно, отражаемого совокупностью обязательных и альтернативных событий, характеризующих выполнение ведущих к цели плановых мероприятий во взаимодействии и последовательности, определяемыми сетевой моделью выполнения задачи. В результате командному и руководящему составу становится доступным во всем объемеи полноте поле управленческой деятельности по оценке обстановки, выработке замысла, принятию решения, организации, координации и контролю подчиненной структуры для его выполнения.

Принципиально важно отказаться от каких-либо автоматических процедур принятия решений – области творческой деятельности человека, высшего уровня управленческой деятельности командного и руководящего состава кораблей и судов. Автоматические процедуры возможны и необходимы в системах управления техническими объектами с детерминированным и стохастическим миром причинно-следственных отношений. Проблемы неточности (случайности, стохастичности) и нечеткости (по Задэ) решаются с применением вероятностно-статистических методов и теории нечетких множеств. Наряду с неточностью и нечеткостью различают еще один аспект неполноты информации – неопределенность или незнание – сферу принятия решений человеком и только человеком. По этой причине подсистема или задача организационного управления выполнением задач из управленческих функций принципиально ограничивается функцией только информационной поддержки.

Эти обстоятельства диктуют необходимость оснащения перспективных систем управления подсистемой или задачей, имеющей общесистемный характер и смысл «Сетевая система автоматизированной поддержки макроуровневого организационного управления выполнением задач … (управления кораблем, судном, боевого управления, управления техническими средствами, борьбой за живучесть)». Рассмотрены основные аспекты разработки этой подсистемы или задачи на основе сетевой информационной технологии.

По мере выполнения мероприятий, от исполнителей или исполнительных датчиков поступают сигналы о выполнении текущих плановых мероприятий, и соответствующие вершины становятся белыми. Представляется очевидным, что при управлении большими и структурно сложными объектами поддержка управленческой деятельности командного и руководящего состава с использованием сетевых планов, реализуемых ПК АСМ АРБИТР, является целесообразной.

Равин А.А., Хруцкий О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ЭВОЛЮЦИЯ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ СУДОВОГО ОБОРУДОВАНИЯ

Анализ потока отказов и аварий судового и корабельного энергетического оборудования свидетельствует о том, что, несмотря на постоянное совершенствование схемных и конструктивных решений, применение прогрессивных материалов и технологий изготовления,

эксплуатационная надёжность наиболее нагруженных и ответственных узлов оборудования оставляет желать лучшего. Кардинальное решение этой проблемы связано с расширенным внедрением в практику эксплуатации судовой энергетики информационных технологий, и в том числе, диагностических систем, обеспечивающих контроль и прогнозирование фактического технического состояния оборудования

Стремление координировать управляющие воздействия в соответствие с достоверной оценкой степени выполнения оборудованием заданных эксплуатационных режимов привело к организации контроля теплотехнических параметров, сначала с помощью приборов теплотехнического контроля, размещённых на местных постах непосредственно в машинных отделениях, затем, по мере развития электрических средств измерения неэлектрических величин, перенесением вторичных измерительных приборов в центральные посты управления (ЦПУ и ПЭЖ).

Необходимостью реализации этой концепции обусловлено последовательное усложнение и усовершенствование систем контроля состояния судового энергетического оборудования, основными этапами которого являются:

—применение приборов контроля, расположенных вблизи объекта на местных постах управления;

—дистанционный централизованный контроль функциональных параметров, необходимых для управления оборудованием;

—расширение номенклатуры контролируемых теплотехнических параметров с целью комплексной оценки работоспособности оборудования;

—применение вычислительной техники в качестве средства сбора и обработки результатов контроля параметров оборудования;

—применение распределённых микропроцессорных структур информационно-вычислительных комплексов;

—включение систем централизованного контроля энергетического оборудования в состав комплексных систем управления техническими средствами (КСУ ТС), а затем и в состав интегрированных систем управления (ИСУ) кораблём;

—совершенствование средств представления информации;

—применение систем информационной поддержки персонала (СИП) и алгоритмов автоматизированной обработки результатов контроля теплотехнических параметров;

—разработка и применение специальных диагностических датчиков и приборов, предназначенных для измерения параметров физических полей, сопровождающих функционирование оборудования, с целью раннего обнаружения развивающихся эксплуатационных дефектов;

—организация на базе измерительных каналов, контролирующих теплотехнические и специальные параметры, сначала локальных, а затем и комплексных систем технического диагностирования (СТД) судовых технических средств.

Для эффективной и безопасной эксплуатации СЭУ требуется обеспечить обслуживающий персонал комплексной информацией о состоянии энергетического оборудования и протекающих в них технологических процессах с помощью систем централизованного контроля, которые осуществляют функции измерения параметров и сравнения их с установками. При предельном отклонении контролируемых параметров обеспечивается срабатывание звуковой и световой АПС (входит в состав СЦК), регистрация параметров или факта их отклонения. СЦК состоят из датчиков, электронных приборов (элементов обработки сигналов и средств отображения, регистрации, сигнализации и, как правило, имеют обегающий принцип действия. В качестве примера такой СЦК можно указать отечественную систему «Шипка-М».

В докладе авторами рассмотрены варианты структурной организации СЦК разных поколений.

Показано, что расширение функциональных возможностей более поздних модификаций судовых СЦК обеспечивалось за счёт применения более эффективных средств обработки и представления информации на базе вычислительной техники (централизованных компьютеров и микропроцессоров) и расширения номенклатуры и функционального назначения датчиков.

Использование вычислительной техники в составе СЦК повысило эффективность и надёжность сбора, обработки, хранения и представления информации и создало условия для объединения систем централизованного контроля с близкими по принципу действия системами аварийно-предупредительной сигнализации, системами автоматической защиты, системами автоматического управления и впоследствии, и с системами технической диагностики. Благодаря применению на судах микропроцессорной вычислительной техники, получили распространение системы с распределенной структурой, а разработка специальных алгоритмов и активных мнемосхем создала условия для внедрения систем информационной поддержки персонала (СИП) которые явились предтечей комплексных систем технической диагностики, призванных обеспечить повышение эксплуатационной надёжности оборудования.

Разживин Н.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ИНФОРМАЦИОННЫЕУЯЗВИМОСТИИ УГРОЗЫ ВОДИТЕЛЯПРИ РЕШЕНИИЗАДАЧ НАВИГАЦИИ

Глобальная система позиционирования уже настолько прочно вошла в жизнь современных компаний и корпораций, что владельцам и сотрудникам сложно представить, каким образом без технологий GPS можно обойтись при решении повседневных задач. Растут и развиваются многочисленные сервисы, и уже многие автоматизированные системы, работающие практически без вмешательства человека (автоматически), принимают, как правило, даже без сомнений за основу данные, получаемые от спутников. Однако, в последнее время к безопасности использования средств GPS-мониторинга накопилось достаточно много вопросов.

В настоящее время известна угроза, связанная с искажением информации о пробках на дорогах, передаваемой на автомобильные системы по радиоканалу, используя международный протокол. При этом информация о текущем местоположении транспортного средства, определяемая установленным в нем GPS-приемником, не искажается. В ряде случаев злоумышленники способны парализовать жизнь современного города – например, направляя автомобили в уже существующие пробки и тем самым значительно осложняя нормализацию дорожного движения.

Использование глобальной системы позицирования открывает перед злоумышленниками большое количество уязвимостей для реализации – простой и недорогой антенный комплекс дает хакеру возможность передавать недостоверную информацию о дорожном движении на автомобильные навигационные системы в радиусе 16 км. Фактор уязвимости не зависит от типа спутниковой системы, используемой в системе GPS.

Например, студенты четвертого курса Израильского технологического института смогли осуществить хакерскую атаку на популярное GPS-приложение Waze. Студенты создали виртуальную пробку, продемонстрировав тем самым, что злоумышленники таким образом могут создать аварийные ситуации на дороге, используя уязвимости в системе навигации.

Специалисты из калифорнийской лаборатории Sandia смогли передать ложную геолокационную информацию сразу на несколько сотен тысяч виртуальных мобильных устройств на базе Android.

Совсем недавно произошел инцедентс компанией Яндекс. Навигационное приложение устройств «Яндекс.Навигатор» втайне от владельца записывало все звуки и разговоры, которые улавливал микрофон девайса. Запись прекращалась только тогда, когда на устройстве заканчивалась свободная память. Представители «Яндекса» утверждают, что это была банальная ошибка в обновлении, а так же, что данные никуда не отправлялись.

Такие ситуации и демонстрируют нам о довольно значительной проблеме в навигационных системах, необходимости совершенствования систем обеспечения пользователей.

На сегодняшний день развитие навигации происходит очень быстро, автомобильные навигаторы снабжаются аудио видео записывающей аппаратурой и многими другими функциями которые отнюдь не безопасны для пользователей.

Угрозы могут возникнуть колоссальные по масштабу, так как во многих автомобилях существуют встроенные навигационные системы. Исходя из этого существует возможность не только отслеживать место нахождения автотранспорта, но и получения данных о присутствии пассажиров или владельца в салоне, а также несанкционированного доступа к аудио и видео поддержке.

Не менее важным является реальная угроза жизни, так как встроенная навигация имеет связь с электроникой автомобиля. Злоумышленники могут дистанционно заблокировать руль, что приведет к серьезным дорожно-транспортным последствиям.

Одна из проблем, как нам представляется, отсутствие системного подхода к выполнению работ по обеспечению навигации. Работы выполняются различными организациями, как государственными, так и частными. Единого плана и контроля отсутствия системных ошибок, как следует из анализа некоторых фактов, нет. Это соответственно приводит к дублированию работ, увеличению их стоимости, а также созданию и использованию несертифицированной продукции. Продукции, не гарантирующей соответствующего качества, достоверности данных и безопасности пользователей.

Главным средством защиты в этих случаях на сегодняшний день мы видим в введение системы регламентов и наказаний за генерацию помех GPS сигнала. Если, например, в Австралии за действия, приводящие к нарушению безопасности мореходства, законодательством предусмотрено 5 лет тюрьмы и большой штраф, то в США за создание помех в GPS-сетях злоумышленникам грозит только конфискация используемого оборудования. Это не может восприниматься серьезно.

В России защита навигационных систем осуществляется на основании федерального закона №22 – ФЗ «О навигационной деятельности» и, как следует из анализа, системно в части регламентирования действий (праворегулирования) решена на достаточном уровне, чего нельзя сказать об исполнении принятых регламентов.

Рыжиков Ю.И., Алексеев А.В., Лохвицкий В.А.
Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского,
Институт автоматизации процессов борьбы за живучесть корабля, судна

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ЛУЧЕВЫХ ДИАГРАММ ПРИ ПОЛИМОДЕЛЬНОМ ОЦЕНИВАНИИ И АНАЛИЗЕ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Среди комплекса решаемых проблем управления информационной безопасностью (УИБ) критических объектов, к числу которых в полной мере относятся объекты морской техники и морской инфраструктуры (ОМТИ), особое место традиционно занимает проблема и технологии многокритериального оценивания качества и эффективности используемых технических средств и их систем. Успешное решение данной проблемы и соответствующих задач квалиметрического оценивания с учетом конкретных условий эксплуатации современных сложных средств и систем УИБ (СУИБ) позволяет, как эффективно ими управлять, так и обоснованно формировать в процессе их разработки и внедрения новые требования к СУИБ, синтезировать новые оптимальные технологические решения.

Анализ последних достижений в области квалиметрии сложных организационно-технических систем и, в первую очередь, критических объектов показывает перспективность развития концепции и практик их полимодельного многокритериального оценивания, анализа, синтеза. Именно многоаспектное измерение качества современных СУИБ ОМТИ позволяет всесторонне учитывать специфику их построения, функционирования и использования в условиях критичного влияния широкого спектра угроз, уязвимостей и вариантов их реализации, характерных для задач информационного противоборства, обоснованно решать проектные задачи выбора их структур, функционала и системных параметров.

В свою очередь, концепция полимодельного оценивания предусматривает наличие и применение ряда верифицированных, валидных и сертифицированных методов, технологий и средств оценивания качества анализируемых СУИБ при соответствующих сопоставимых и адекватных условиях. Среди них, по мнению авторов, заслуживают определенного внимания сравнительно новые и разрабатываемые в настоящее время методы и технология лучевых диаграмм (ТЛД).

Существо ТЛД сводится к многокритериальному измерению качества сложных организационно-технических (эрготехнических) систем, в том числе СУИБ ОМТИ, на основе измерения площадей в векторном пространстве, ограниченных соответствующими контурами оценивания отдельных свойств по частным (ЧПК) и групповым показателям качества (ГПК) с соответствующим переходом (скаляризацией) к модельным агрегированным (сводным, интегрированным) показателям качества (МПК).

В свою очередь, скаляризация МПК с использованием ТЛД позволяет перейти непосредственно к оценке агрегированного полимодельного показателя качества (АПК) для последующего решения задач анализа, синтеза и оптимизации параметров средств, проектных и управленческих решений.

В представляемых результатах исследований рассмотрены многовариантные оценки качества основных классов средств УИБ ОМТИ – межсетевых экранов, средств защиты от вредоносных кодов, а также сканеров информационной безопасности типа XPpider (Positive Technologies), Internet Scanner, Ревизор сети, Microsoft Baseline Securite Analyzer, Retina. Кроме того - их комплексов (вариантов комбинированного использования). Оценки выполнены по 12 наиболее представительным (основным) критериям (ЧПК) их качества при использовании 5 моделей предпочтений, а также по 7 моделям оценивания – АСПТИД-3W, КРОПУР, АСОР, МКО, ОИБ, СПРУ-ИБ. При оценках по ТЛД использовался ранее разработанный программный комплекс RCH_Build, адаптированный к решению задач оценки качества средств и систем УИБ ОМТИ (версия о2).

Полученные оценки показали их достаточно приемлемую для практики УИБ ОМТИ сходимость (порядка 15%) по МПК, возможность анализа и учета при принятии комплексных решений специфики используемых квалиметрических методов, технологий и средств поддержки принятия полимодельных решений, а также возможность и необходимость повышения точности задания ЧПК в процессе оценивания за счет их корректировки, дополнительного экспертного оценивания, необходимости обязательной интерпретации получаемых оценок ГПК, МПК, АПК, их верификации и оценки валидности.

Более того, показана возможность существенного повышения достоверности экспертного оценивания качества вариантов СУИБ ОМТИ, например, при квалиметрическом ранжировании средств в ходе решения проектных задач за счет дополнительного представления экспертам матриц многокритериального полимодельного оценивания различных вариантов СУИБ.

В связи с высокой наукоёмкостью и трудоёмкостью решения задач квалиметрического оценивания (ранжирования) критических объектов, в том числе типа СУИБ ОМТИ, в условиях возрастания национальных требований к комплексной безопасности объектов, подтверждена

целесообразность перехода от сертификации соответствия используемых средств к сертификации их качества на основе методов полимодельного многокритериального оценивания.

Более того, подтверждена необходимость квалиметрической аттестации (ранжирования) критических объектов с использованием комплексов квалиметрического оценивания и анализа при разработке соответствующих регламентов и расширении функций федеральных органов по сертификации с созданием специализированных испытательных центров ранговой сертификации.

Савченко Б.В.
Россия, Санкт-Петербург, Санкт-Петербургской государственный морской технический университет

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АЛГОРИТМЫ ПОИСКА ПУТИ ЗАЩИТЫ И ИХ ОПТИМИЗАЦИЯ

В настоящее время развитие компьютерных технологий достигло такого уровня, при котором, например, вредоносные программы (коды) непрерывно становятся все более сложными и неуловимыми. Программы, которые созданы выявлять вирусы и шпионское программное обеспечение (ПО), едва «успевают» за ними. Противодействие вредоносным программам, как правило, использует заложенные в них экспертом алгоритмы действия, которые в ряде случаев неэффективны для защиты от постоянно появляющегося и модернизируемого вредоносного ПО.

Имеет место случай, когда «меч» практически бьет быстрее, чем «щит» встает у него на пути. При этом последствия этого могут быть катастрофичными и необратимыми. А произойти подобная ситуация может, как в масштабах небольшого коммерческого предприятия, так и в масштабах целого объекта информатизации, региона, государства.

Именно поэтому роль искусственного интеллекта при решении задач информационной безопасности сегодня непрерывно повышается: программы, способные обучатся самостоятельно, смогут дольше оставаться конкурентноспособными на рынке защитного ПО.

К тому же, нельзя забывать о том, что для оперативной реакции на угрозу в современных условиях требуется практически мгновенная обработка большого количества информации. Это, безусловно, трудновыполнимая задача даже для группы квалифицированных специалистов. В то же время, искусственный интеллект (ИИ) способен сделать это в разы быстрее, а также качественнее. Потому что использование ИИ практически исключает пресловутый «человеческий фактор» (ЧФ), т.е. негативное влияние субъективных свойств операторов. А, как известно, «магистральным путем» его преодоления является полномасштабная автоматизация процессов, в которых оператор занят.

Главное преимуществосистем с использованием ИИ состоит в их способности к решению аналитических задач и, даже, проведению самостоятельных исследований, накоплению и классификации полученного в результате опыта. Однако, несмотря на эти важные преимущества ИИ, системы с его использованием - трудно реализуемы. По весьма многим причинам, в том числе техническим.

Одной из наиболее важных проблем при этом, является оптимизация алгоритмов поиска пути, которые используются практически во всех сферах деятельности, где применяется ИИ. Ведь задача обеспечения информационной безопасности крайне трудна, требует доведения ИИ до такого состояния, в котором его можно перенастроить, исправить или дополнить. И не стоит забывать о том, что в большинстве случаев, мы имеем дело не с одним компьютером, а с целой сетью, которая может насчитывать десятки и сотни компьютеров. И от возможности найти поврежденный файл, затратив на это минимальное количество времени и ресурсов, зачастую будет зависеть безопасность всей системы и объекта автоматизации в целом.

В докладе приведены и обсуждаются самые «удобные», по мнению автора, алгоритмы поиска пути защиты объектов автоматизации, а также способы их оптимизации, в зависимости от задач. При этом, вариантная оптимизация алгоритмов обеспечения защиты информационных ресурсов непременно требует проведения комплексных оценок качества функционирования объекта информатизации, непрерывного наблюдения (мониторинга) за их изменением, выявления тенденций к изменению (трендов) и прогнозирования ожидаемых значений. Причем, обязательно в автоматическом режиме и с цветовой безизбыточной визуализацией для минимизации психофизиологической нагрузки на операторов.

Показана реализуемость этих способов и доступность для внедрения в различные сферы человеческой деятельности. Кроме того, показаны потенциально новые возможности системы, как в нахождении вредоносного ПО, так и в других задачах ИИ.

В заключении отмечается, что искусственный интеллект представляет собой будущее компьютерных технологий и решение проблем, связанных с оптимизацией конкретных составляющих искусственного интеллекта. Это позволит освободить часть ресурсов системы, а также обеспечит начало движения в сторону модернизации и улучшения искусственного интеллекта. Более того, повысит устойчивость систем, где он применяется к воздействию вредоносных программ.

Салащенко А.И., Леберянский А.П.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНЫХ ЛОДОК

В процессе использования и эксплуатации атомной подводной лодки, ее живучесть обеспечивается тремя составляющими:

–конструктивными мероприятиями;

–организационно-техническими мероприятиями;

–действиями личного состава по борьбе за живучесть.

Реализация всех трех составляющих живучести атомной подводной лодки, в конечном счете, зависит от уровня подготовки личного состава к обеспечению живучести корабля в повседневных условиях, а при возникновении боевых и аварийных повреждений - к борьбе за его живучесть. Исследование аварийности в ВМФ показывает ее значительный рост и высокий процент вины личного состава в этом. Поэтому даже ни высокое конструктивное обеспечение живучести атомной подводной лодки, ни большое количество разработанных организационно-технических мероприятий не снизит уровень аварийности и не обеспечит успех борьбы за живучесть при возникновении аварийной ситуации, если не будет достаточно хорошо подготовлен личный состав в вопросах обеспечения живучести атомной подводной лодки.

Особое значение в обеспечении живучести ПЛА имеет уровень подготовки офицеров, их умения организовать на корабле выполнение организационно-технических мероприятий по обеспечению живучести, а в случае возникновения аварийной ситуации грамотно руководить борьбой за живучесть.

Под руководством борьбой за живучесть следует понимать циклично повторяющийся процесс воздействия руководителя борьбы за живучесть (органа управления) на управляемый объект (корабль, как сложное инженерное сооружение, отсек, комплексы оружия или технических средств и экипаж или подразделение с установленной организацией), в котором (в процессе) 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 (действий) 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.

Происшедшие с атомными подводными лодками ВМФ катастрофы и тяжелые происшествия показывают, что большинство из них могли бы быть предотвращены или локализованы и ликвидированы без тяжелых последствий при грамотных действиях хотя бы одного из должностных лиц находящихся на мостике, главном командном пункте корабля или командных пунктах боевых частей и служб. Но в результате своей слабой подготовки, эти должностные лица оказались неспособными оценить опасность возникшей ситуации, предотвратить ее развитие и выполнить грамотные действия по руководству борьбой за живучесть.

Одной из основных причин такого результата подготовки является несовершенство существующей в ВМФ системы подготовки офицеров ПЛА к руководству борьбой за живучесть.

В настоящее время проблеме обеспечения живучести ПЛА, а также отдельным ее аспектам посвящено много работ. В большей части они посвящены научному аспекту живучести, перед которым стоит задача разработки теории живучести объектов и технических систем. Первоочередной задачей теории является разработка методов количественной оценки риска возникновения той или иной аварии и прогнозирование ее возможных последствий. Наиболее трудным препятствием на пути создания этой теории является огромный перечень всех ситуаций, которые могут привести техническую систему в более опасное состояние, и малый объем статистического материала.

Обеспечение безопасности сложных организационно-технических систем является предметом специальных научных исследований. Эта задача стоит перед проектировщиками и строителями атомных подводных лодок, а также перед организациями, их эксплуатирующими. Сложность проблемы заключается в том, что корабль может быть построен в полном соответствии с существующими требованиями, но, тем не менее, попасть в катастрофу, т.к. обстоятельства, явившиеся причиной аварии, не были и не могли быть предусмотрены. Снижение риска в использовании кораблей по назначению может быть достигнуто только на основании системного подхода.

Среди методов исследования аварийных ситуаций наиболее разработанными являются методы, основанные на теории графов и алгебры логики. Сущность этих методов заключается в том, что на основе тщательного и конкретного анализа объекта и физики воздействия на него неблагоприятных факторов определяются все возможные опасные состояния системы, затем выявляются причины, которые могут привести к катастрофе. По каждому опасному состоянию ведется анализ отказов ее конструктивных элементов или цепочки отказов до тех пор, пока не будет найден выход из строя конкретного узла, инициирующего отказ элемента. В результате такого подхода строится так называемое «дерево отказов» или логические функции.

Для практического использования этих методов исследования аварийных ситуаций необходимо максимально конкретизировать и сформулировать суть опасного состояния, ограничить объект исследования разумными пределами, использовать строгую логику и тщательность перебора возможных ситуаций для составления сценария развития событий, переводящих систему в более опасноесостояние. Такой анализ можно вести как «снизу вверх», т.е. от опасного состояния до инициирующего события, так и «сверху вниз» от первоначальной причины к опасному состоянию.

Для моделирования опасного состояния, как правило, используются графоаналитические, вероятностные и логико-вероятностные модели. Они позволяют объективно выявлять наиболее опасные объекты, причины возникновения опасных ситуаций, условия, влияющие на дальнейшее развитие событий в опасном направлении, характер развития событий во времени и другие обстоятельства, способные повлиять на безопасность людей. Наиболее эффективными для использования являются логико-вероятностные модели, пригодные не только для технических, но и для организационно-технических систем.

Сергейчик М.В.
Россия, Санкт-Петербург, ОАО «Концерн «НПО «Аврора»

АЛГОРИТМ УПРАВЛЕНИЯ СКОРОСТЬЮ ПЕРЕКЛАДКИ РУЛЕВЫХ УСТРОЙСТВ ОТ СИСТЕМ УПРАВЛЕНИЯ ДВИЖЕНИЕМ И ЕГО ИНФОРМАЦИОННАЯ ЗАЩИЩЕННОСТЬ

Рулевые устройства (РУ) с гидроприводом для морских подвижных объектов (МПО) предыдущих поколений имели в своем составе необходимый набор регулировочных гидравлических приборов - дросселей для обеспечения режимов работы. При этом управляющие электрогидравлические приборы, входящие в СУД, в процессе перекладки рулевых устройств работали в релейном режиме.

При создании гидравлических устройств и приборов для МПО нового поколения пришлось отказаться от релейного регулирования, а для настройки необходимых скоростей перекладки перейти на работу с электрогидравлическими приборами – распределителями золотникового типа с пропорциональным управлением.

При этом существенные технологические разбросы параметров электрогидравлических приборов с пропорциональным управлением, погрешности, вносимые электронными устройствами – модулями в формируемый сигнал управления гидроприводом, приводят к необходимости индивидуальной настройки каналов управления. Это делает процесс регулировки весьма трудоемким и, к сожалению, не исключающим ошибки операторов при регулировании. Информационной угрозы, обусловленной пресловутым «человеческим фактором». Для её исключения, а также снижения трудозатрат регулировочно-наладочных работ и отработки СУД и РУ на МПО предлагается к применению алгоритм следящего управления, работающего в зоне частичных открытий золотниковых распределителей, инвариантного к разбросу параметров. Причем, как каналов управления СУД, так и объектов регулирования в целом. Более того, в информационно защищенном исполнении.

Предлагается два варианта управления распределителями и нейтрализации ошибок операторов.

В первом варианте организован контур управления по позиционно-дифференциальному (ПД) типу алгоритма управления. Этот контур является вложенным для контура управления РУ, который также управляется по ПД - принципу (двухконтурный ПД-алгоритм управления). Входными сигналами контура управления перекладкой являются сигналы о заданном и текущем положении РУ. Выходным сигналом является сигнал заданного положения прибора - распределителя, который подается на вход контура позиционирования распределителя.

Сигнал о текущем положении РУ поступает в контур управления от прибора обратной связи через преобразователь типа, например, резольвер, преобразующий угол разворота вращающихся трансформаторов в приборе обратной связи в цифровой код. Первая ветка контура работает в зоне малых рассогласований и обеспечивает пропорциональное управление распределителя от рассогласования заданного значения в сравнении с текущим. Во второй ветке реализован ПД-алгоритм управления. Он работает на больших рассогласованиях, когда РУ разгоняется до заданного значения угловой скорости и стабилизирует эту скорость на всем участке перекладки.

Статическая ошибка стабилизации скорости перекладки зависит от величины заданных коэффициентов. Чем выше значения, тем выше добротность контура и меньше ошибка.

Переключение между пропорциональным и скоростным управлением организовано таким образом, чтобы в момент переключения избежать броска распределителя, т.е. чтобы расчетные значения сигналов в первой и второй ветвях прохождения сигнала были равны. Вычисленное заданное положение распределителя подается на вход контура позиционирования. Тем самым, в контуре управления формируется ПД-алгоритм. Вычисленный сигнал управления с широтно-импульсной модуляцией подается на гидравлический прибор, где и позиционирует в заданном положении распределителя. Сигнал о положении распределителя от вращающихся трансформаторов через преобразователь «угол – код» подается на вход контура в качестве сигнала обратной связи по положению распределителя. Для реализации приведенного алгоритма необходимо применение аппаратно-программных средств и программного обеспечения с малыми циклами обработки информации в режиме реального времени.

Во втором варианте предполагается не выделять контур управления распределителя, а контур управления РУ организовать по позиционно-дифференциально-дифференциальному типу (одноконтурный ПДД-алгоритм управления), т.е. с использованием первой и второй производной по положению РУ.

Отличие заключается во введении в контур управления второй производной по РУ и отсутствии контура позиционирования распределителя. Сигнал задания положения распределителя в этом случае подается непосредственно для преобразования в ШИМ-сигналы и управления распределителем.

Такой алгоритм является более предпочтительным, т.к. несет более полную информацию о конечном объекте управления.

Сухов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СИСТЕМА ВИЗУАЛЬНОГО УПРАВЛЕНИЯ АВТОМАТИЗИРОВАННЫМИ УСТРОЙСТВАМИ

Технология компьютерного зрения считается одной из самых передовых и перспективных на этом этапе истории. К сожалению, в современной литературе с трудом удается отыскать информацию по данной тематике. Большинство опубликованных текстов раскрывают не саму суть технологии, а просто описывают отдельные вопросы, опуская наиболее интересные и важные из них. Как правило, все сводится к описанию какого-либо приложения или группы приложений.

Вот уже несколько десятилетий проблема машинного зрения занимает умы не только исследователей, но и тех, кто связан с современным высокотехнологичным и высокотехническим производством. Совершенствование персональных вычислительных машин, увеличение производительности компьютеров и появление на рынке недорогих устройств ввода видеоинформации существенно стимулируют данную область. При этом, уже сейчас становится ясно, что от успешного решения ряда сложных и неоднозначных задач компьютерного зрения зависит автоматизация множества процессов и операций, которые до этого управлялись и контролировались только человеком.

Область использования компьютерного зрения и в области морских комплексов весьма широка. На данный момент основным потребителем разработок компьютерного зрения и обработки визуальной информации является сфера развлечений. Это объясняется огромными финансами,приходящимися на видео-развлечения. И это стимулирует серьезное развитие, как высоких технологий в целом, так и искусственного зрения в частности.

Однако, использовать достижения компьютерного зрения возможно и в промышленности, и в комплексах специального назначения. Сейчас, во время модернизации технологий, все больше обязанностей «перекладывается» на роботов или роботизированные системы. И для улучшения их работы используются различные технологии, включая технологию компьютерного зрения.

Предлагаемая к анализу Система визуального управления автоматизированными устройствами (СВУАУ), как раз относится к таким технологиям. Используя в основе своей работы отечественную библиотеку, позволяющую работать напрямую с видеокамеройOpenCV, СВУАУ представляет инструмент для работы с визуально изменяющимися данными. Данная библиотека включает в себя широкий перечень возможностей для анализа цвета, видеопотока и многое другое.

Существо технологии СВУАУ состоит в распознавании сигналов, подаваемых оператором с помощью маркера, который может автоматически определятся. Эти сигналы представляют собой контуры, заранее внесенные в базу данных. Возможности системы позволяют динамически добавлять контуры в базу и использовать одновременно несколько маркеров. Данный подход позволяет использовать увеличенное количество контуров. Это соответствует большему количеству команд, которые можно подавать приемнику информации, для дальнейшего исполнения.

СВУАУ предназначена для использования на производствах, в которых есть необходимость использования автоматизированных систем, но при этом использование пульта управления ограничено в связи с неудобством, дороговизной.

Такое производство возможно, к примеру, в отраслях, где человек работает совместно с роботом. Работа в сфере фармакологии и исследований опасных веществ, производство микроэлектроники. При данной работе возможно использование роботизированной «руки», которая оказывает различную помощь. Такая помощь может выражаться в удержании пробирки с веществом, очистке рабочей среды, других действиях с использованием преимуществ роботизированной руки. Данная технология удобна в использовании в боксах бактериальной воздушной среды. Такие боксы широко используются при работе, когда нужно минимизировать контакт с внешней средой. Обычно они оснащены перчаточными портами, и когда руки оператора находятся в портах достаточно сложно управлять пультом. А так как в данных лабораториях и производствах должна быть тишина, голосовое управление не возможно. В этом случае подача сигналов маркером является выходом из возникшей проблемы.

Тарабаров А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВ АВТОРИЗАЦИИ И ВОЗМОЖНОСТЕЙ ИХ СОВЕРШЕНСТВОВАНИЯ

Уязвимости высокого уровня риска в программном коде, а также серьезные недостатки механизмов аутентификации и авторизации во многих системах позволяют проводить несанкционированные действия или даже получить полный контроль над информационно-коммуникационной системой со стороны, как внутреннего, так и внешнего злоумышленника.Это, как показывает практика, может привести к существенным материальным,репутационными другим видам потерь.

Авторизация (от английского «Authorization»), как известно, понятие, изначально использовавшееся в банковской сфере, в области платежных карт и означает процедуру идентификации лица для предоставления доступа к неким ресурсам или возможностям, имеющим ограниченный доступ.Авторизация пользователейиспользуется для предоставления доступа к базам данных в защищенном исполнении; для получения прав добавления сообщений на форуме, размещения пресс-релизов на ленте новостей и т.п. возможностям, предназначенным для ограниченной группы пользователей.

Традиционно, процедура авторизации заключается в введении пользователем в специальную форму своих уникальных идентификационных данных - логина и пароля. Далее эти данные проверяются на наличие в базе данных пользователей соответствующего информационного ресурса, и определяется, к какой категории относится данный пользователь. В результате процедуры авторизации пользователь получает, либо не получает необходимый доступ. Логин и пароль ранее должны быть получены пользователем в результате процедуры регистрации на данном ресурсе. Нередко, зарегистрировавшись на некотором сайте, пользователь в дальнейшем теряет свои регистрационные данные. На этот случай на сайте должна быть предусмотрена удобная процедура восстановления пароля.

Многие современные системы имеют уязвимости сервисов авторизации с весьма высоким уровнем риска. Большая часть уязвимостей сервисов авторизации связана с ошибками реализации механизмов защиты систем, допущенных разработчиками. К данной категории уязвимостей относятся недостатки механизмов идентификации, аутентификации и авторизации. Остальные уязвимости в основном связаны с недостатками конфигурации.

При определенных уязвимостях в коде, если пользователь перейдет по специально сформированной вредоносной ссылке, атакующий может получить доступ к системе с привилегиями данного пользователя. Часто в системах встречаются уязвимости, связанные с предсказуемыми форматами идентификаторов пользователей.

Распространены также уязвимости, позволяющие реализовать атаки на сессии пользователей. Уязвимости, связанные с некорректным завершением сессий, некорректной настройкой cookie-параметров, возможностью параллельной работы нескольких сессий для одного пользователя, отсутствием привязки сессии к IP-адресу клиента и др. При успешной атаке злоумышленник может получить доступ к личному кабинету пользователя с его привилегиями.

Так же существуютопасные уязвимости высокой степени риска, в результате которых злоумышленник может получить содержимое файлов, хранящихся на уязвимом сервере, данные об открытых сетевых портах узла, вызвать отказ в обслуживании всей системы, а также, в ряде случаев, обратиться к произвольному узлу от лица уязвимого сервера и развить атаку.

Большинство распространенных уязвимостей имеет средний или низкий уровень риска. Тем не менее, в сочетании с особенностями функционирования конкретных систем это может привести к реализации серьезных угроз безопасности, включая кражу конфиденциальных, коммерческих или персональных данных.

Часто недостатком механизмов идентификации и авторизации является предсказуемость формата идентификатора учетной записи. Зная несколько существующих в системе идентификаторов, злоумышленник может вычислить механизм их формирования и подобрать нужный. Так же недостатки реализации имеют механизмы аутентификации, например, слабую парольную политику, недостаточную защиту от подбора учетных данных, возможность обхода механизма CAPTCHA или отсутствие обязательной двухфакторной аутентификации при входе в личный кабинет.

Таким образом, пока пользователи современных информационно-коммуникационныхсистем допускают ошибки в организации безопасности, помогая злоумышленникам находить новые пути обхода защиты информации, вопрос решения проблем авторизации будет актуальным.

Тобольченко А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской техническийуниверситет

ПРАКТИКА СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРИ РЕШЕНИИ ЗАДАЧИ О НОРМИРОВАНИИ ИТОГОВЫХ ПОКАЗАТЕЛЕЙ СИСТЕМ УПРАВЛЕНИЯ СО СТАТИСТИЧЕСКОЙ НЕПОЛНОТОЙ

При рассмотрении задачи прогнозирования систем со статистической неполнотой, не сложно заметить ситуацию, при которой найденное математическое решение может быть не только довольно сложным, но и вариативным.

Естественно, в условиях использования систем с ограниченным по времени циклом принятия решения, может оказаться невозможно тратить время на расчеты и обдумывание полученных результатов. Особенно это будет критичным в случае, когда прогнозируемый ряд имеет тенденцию к расхождению – тут оператор будет ограничен уже даже не самим циклом принятия решения, но даже более того – тенденцией корректирующей величины к неконтролируемому росту.

Может возникнуть и обратная ситуация, если прогноз попадает в бифуркационное поле и может качественно меняться в зависимости от момента вмешательства оператора. В этом случае, оператор не только должен уложиться в срок принятия решения, учитывая требования самой системы управления, но и произвести все расчеты и принять решение до того момента, как корректировка будет качественно изменена. Более того, второй случай намного более сложен и может поставить в тупик, даже очень опытных специалистов, привыкших за многолетнюю практику быстро принимать взвешенные решения. Это обусловлено тем, что по факту, оператор должен произвести не один, а сразу несколько расчетов, оценивая каждое качественное изменение систему в допустимый период внесения корректировки и только потом произвести выбор, опираясь уже на ряде прогнозов, так как ситуация, при которой более эффективным решением будет дождаться изменения качественного уровня корректировки и только потом предпринять необходимые действия – является наиболее вероятной.

Как же можно помочь оператору в данной ситуации? Кажущееся очевидным решение о создании программного вычислительного комплекса, способного производить необходимые расчеты – на самом деле является только частичным решением и снимает с оператора необходимость самих вычислений, но мало чем помогает в оценке и принятии решений.

Таким образом, единственным реальным решением будет создание интеллектуального помощника, который бы автоматизировал процесс расчетов, при этом без участия оператора производил бы сбор и подготовку информации для них, и участвовал бы в анализе результатов, помогая определить эффективность внесения изменений не только в данный момент времени, но представляя прогноз аналогичной картины для будущих моментов, потенциально важных для участия оператора.

Такой подход позволяет предоставить оператору не срез, а динамику как реальной ситуации, так и необходимых корректировок и спрогнозированых измененных состояний системы.

Важно отметить, что интеллектуальная составляющая такой системы крайне важна по нескольким причинам:

– в связи с высокой вариативностью расчетов, предоставление сухого результата будет малоинформативно и не позволит оператору быстро и уверенно принять решение. Остро стоит вопрос о “рекомендациях” для оператора или (что имеет большее значение при развитии системы) о “маркерах” – т.е. системы дифференциации информации в расчетах таким образом, что бы выделять параметры, которые для данного среза имеют наиболее большое значение (важно, что ранжирование значимости параметров в срезах – это отдельная задача интеллектуального помощника и она открывает большой горизонт развития данной технологии)

– в связи с тем, что каждый оператор имеет свой подход к принятию решений, необходимо, что бы система учитывала это, подстраиваясь под каждого конкретного оператора с учетом его метода работы. Сложно переоценить данную задачу, так как по нашим наблюдениям, более 80% времени работы оператора могут быть потрачены на его “борьбу” с навязанными ему методами работы.

– производя прогнозирование системы со статистической неполнотой, важно помнить о том, что расчеты заведомо содержать определенный процент погрешности, который так же надо учитывать при принятии решения. К сожалению, невозможно однозначно определить его влияние на итоговый результат, так как погрешность изначальных вычислений может быть как скомпенсирована вариативностью прогноза, так и усилена. Однако, можно использовать метод двойной встречной проверки и через построение регрессии, выявлять отклонение итогового среза от прогнозируемого. Этот нечеткий параметр может быть только показателем надежности (“доверенности”) произведенных расчетов и уже в адаптированной форме его можно вывести оператору для каждого предполагаемого действия, уточняя таким образом рекомендацию. Очевидно, что данная задача не сводится только к расчету показателя, но требует еще и способности системы обучатся, накапливая статистику расчетов и принятых решений, сравнивая ее со статистикой результатов, с тем что бы выстраивать более точный метод рекомендаций для каждого оператора в отдельности.

Тобольченко А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ СО СТАТИСТИЧЕСКОЙ НЕПОЛНОТОЙ

Одной из основных проблем при решении задачи управления систем с нелинейной динамикой развития, является их свойство стаистической неполноты.

Любой, кто сталкивался с этим явлением понимает, насколько катастрофически может начать расти погрешность прогноза даже при минимальных изменениях управляющих параметров.

С другой стороны, по сути, данные системы мало чем отличаются от других систем управления и так же нуждаются в прогнозировании, без которого практически невозможно с ними работать, ведь без составления прогноза, оператор действует наугад, пытаясь скорректировать управляемый процесс.

Предложенные в конце 80х годов методы поиска экстремумов и сведение через них задачи к дискретному виду, безусловно, помогают при работе с системами имеющими даже большую степень неполноты, но только при условии, что нарушение целостности статистики будет иметь малые, относительно равномерно распределенные интервалы, что очевидно является вырожденным случаем, возможным либо при искусственном преобразовании дискретной системы к непрерывному виду, либо при регулярном внешнем воздействии, либо при наличии собственного биения системы.

С другой стороны, можно рассматривать возможности предложенного в 90х годах метода формирования исключающей маски, позволяющей составить фазовый портрет процесса. Этот метод позволяет намного проще производить анализ системы управления, но по сути просто отбрасывает пробелы в статистике, как не несущие значимой информации. Можно считать этот метод достаточно достоверным, так как, он показывает взаимосвязь отсутствующих частей статистики с присутствующими, что позволяет вывести их грубую оценку и локализовать, относительно всей картины в целом.

К сожалению и этот метод не лишен недостатков:

– разумеется, он так же малоэффективен в случае появления большого непрерывного периода статистической неполноты (причем даже частичной!)

– он не может быть использован к системам имеющим (штатно) разрывы второго рода

– он имеет высокую степень погрешности при синхронных разрывах первого рода, так как они могут быть обобщены между собой

– он крайне уязвим в системах с неравномерным внешним воздействием

Таким образом,оба эти методы хорошо подходят для систем, оценка которых достаточно эффективно проводится и экспертным методом, но мало применимы для целого класса систем, имеющих большую непрерывную неопределенность.

Однако, именно системы имеющие большой период неопределенности, зачастую, представляют наибольший интерес.

Сложно представить себе системы более остро нуждающиеся в прогнозировании,так как именно к этим системам относятся все системы многоуровневого прогнозирования.

В таком случае, возможен метод, позволяющий заменить полный прогноз, определением отдельных параметров с наперед заданной точностью.

Такими параметрами удобно брать усредненные показатели за период, таким образом мы можем одновременно получить и достаточно точный и достаточно показательный прогноз даже для систем с большим периодом статистической неопределенности. Более того, важно отметить, что в этом случае мы получаем не разовый, а непрерывный прогноз на весь период статистической неполноты, что крайне важно при разработке инструментов корректировки и управления системой.

Итоговый результат позволяет иметь актуальную динамику корректирующий воздействий для каждого варианта развития событий, что, в свою очередь, позволяет производить вариативный

многоуровневый анализ сразу нескольких прогнозов, что позволяет добиться более высокой точности прогнозирования (при корреляционном анализе на выявление погрешности) и быстрее находить оптимальный (по заданной функции цели) алгоритм управления.

Однако, даже такой метод таит в себе не мало подводных камней. Основным из них является то, что мы не можем наперед рассчитывать даже усредненные параметры. Вместо этого, нам необходимо произвести сначала грубый расчет прогноза, после чего, регрессионным методом выстроить гипотезы существующих тенденций в нашей модели, дальше явным образом задать несколько наиболее показательных частных случаев (метод определения показательных частных случаев основывается на подходе весового контроля), обобщив которые мы можем вывести общее решение и уже для него сделать условный расчет,заменив статистические коэффициенты на фиксированные определенные нами с точностью до заранее заданной допустимой погрешности.

Таким образом, хотя этот метод и позволяет получать достоверный и показательный результат, тем не менее, необходимо заметить, что мы получаем лишь приближенное частное решение, которое будет требовать повторного составления даже при небольших корректировках значений имеющейся статистики (но зато довольно устойчиво при дополнении статистики, в т.ч. к уменьшению периода статистической неполноты).

Тобольченко А.С., Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ИСПОЛЬЗОВАНИЕ ПОДХОДА ГРУППОВОГО (ВЕСОВОГО) КОНТРОЛЯ ПРИ ОРГАНИЗАЦИИ СИСТЕМЗАЩИТЫ ИНФОРМАЦИИ МЕТОДАМИ ИНФОРМАЦИОННОЙ МАСКИРОВКИ И ДЕЗИНФОРМАЦИИ

На сегодняшний день каждое крупное предприятие уже столкнулось с проблемами организации, как физического, так и информационного барьера, необходимого защитить не только хранящуюся информацию, но и (что иногда даже важнее) защитить рабочий процесс, как внутри, так и вне компании. Разумеется, уже разработано немало технологий, позволяющих организовывать системы защиты информации. В их реализации участвуют многие организации, а выделяемые на это бюджеты могут быть весьма значительными.

Среди реализуемых при этом методов: физическое обособление инфоцентров, разграничение доступа в компьютерных сетях, идентификация сотрудников и ресурсов информационной системы, аутентификация пользователей по предъявляемым ими идентификаторам, а также маскировка информации и многое другое. Однако, первостепенными объектами защиты, прежде всего, являются хранилища данных – сервера, файлохранилища, архивы. И большинство разработанных методов ориентированы именно на защиту хранящейся в них информации. Но есть еще потребность в защите информации, находящейся в процессе подготовки и обработки. Причем, зачастую, эта информация может частично или полностью находиться в ограниченном или общем доступе с клиентами, субподрядчиками, контрагентами, аудиторами и наблюдателями и т.д.

Таким образом, мало того, что сама задача защиты становится на порядок сложнее, так как становится намного сложнее определить “нормальный”, т.е. допустимый режим работы с информацией, сложно сегментировать информацию, отслеживать косвенные утечки и т.д. Но и ко всему прочему добавляется необходимость учета динамики работы с информацией: сама система, которую необходимо защищать, может качественно изменяться с течением времени, расширятся, обновляться и менять состав рабочих групп.

Само по себе усложнение задачи защиты информации, в целом решаемо, путем развития существующих технологий и подходов. Например, недавно корпорация IBM представила программное обеспечение, предназначенное для маскировки закрытых данных. Для того, чтобы сторонние администраторы или разработчики могли без проблем работать в корпоративных системах, но не имели доступа к закрытым данным. Однако, непрерывный мониторинг и переопределение защищаемой системы многократно увеличивает потребность в ресурсах, таких как вычислительные мощности и количество необходимых операторов или модераторов.

Одним из подходов, позволяющих оптимизировать такую нагрузку является метод весового контроля. При исследовании этой задачи оказалось возможным представлять существующее инфополе не как набор информации, а как взаимодействие функциональных групп. Определив всю используемую информацию, как набор единичных высказываний, относящийся к сочетанию определенных функций, авторы смогли получить инструмент, выполняющий одновременно две важные задачи: индексацию и систематизацию информации в любом инфополе. При этом задача индексирования решается автоматически, так как мы получаем только ограниченное количество векторов, однозначно определяющих как назначение группы, так и содержание информации, в нее входящей. Таким образом, имеет место упрощение схемы, отражающей структуру всего инфополя и позволяющую однозначно определить путь к любому высказыванию или информационной группе, оперативно получить доступ на изменение/блокировку или иное управление ими.

Так, деление информации на группы значительно упрощает задачу маскировки информационного поля и, в то же время, делает этот метод еще более надежным. Каждой конечной группе присваивается свой уникальный алгоритм, который может подвергаться быстрому изменению при необходимости. При этом, появление возможной уязвимости и, как следствие, угрозы в одной из групп не влияет на информационное поле в целом и не дает злоумышленнику доступ ко всей информации. Задача систематизации так же решается естественным образом при составлении такой структуры, так как каждая группа оказывается явным образом описанной конечным вектором, позволяющим определить ее релевантность всему набору существующих в данной системе критериев. Это позволяет обеспечить удобный поиск информации, определение ключевых изменений инфополя, поиск потенциальных уязвимостей, и более эффективное точечное (а не ко всей системе) применение мер информационной защиты.

В процессе работы было обнаружено, что дополнительно данный метод предоставляет еще и возможность ранжирования функциональных и информационных групп, как по формальным признакам, так и в ручном режиме по оценке эксперта. По мнению авторов, сложно переоценить такой мощный инструмент, позволяющий совершать сколь угодно гибкую настройку комплексной системы информационной защиты.

Благодаря этому методу, авторы смогли существенно снизить сложность задач по информационной маскировке и разграничению доступа. Отдельно рассмотрены механизмы выявления потенциально уязвимых инфоузлов и создание дезинформации, способной снизить степень угрозы. Например, отвлечением внимания или смещением интереса потенциальных злоумышленников от реально значимой информации. Или защитить информацию, искажая ее. В данной задаче, метод весового контроля оказался весьма эффективным, так как позволяет в реальном времени отслеживать не только структуру информационного поля, но и наиболее приоритетные его составляющие.

Туркин И.И.,Мин Хеин
Россия,Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ОСОБЕННОСТИ АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЖИВУЧЕСТИ СУДОВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Успех в применении систем управления с микропроцессорными элементами зависит от нескольких факторов: достигнутого уровня развития теории управления, степени разработанности вычислительных методов для реализации алгоритмов управления, состояния и возможностей вычислительной техники, наличия прикладных методов проектирования. Устранение разрыва между уровнем развития теории управления, алгоритмов и методов их программного завершения, средств реализации, с одной стороны, и возможностями использования этих результатов для решения задач повышения эффективности автоматизации различных объектов, с другой, является одной из актуальных задач первостепенного значения. При наличии такого разрыва современные судовые системы управления объектами различного назначения с ЭВМ, в том числе для обеспечения живучести, не могут быть использованы эффективно. Большинство судовых технических средств (СТС) следует отнести к сложным объектам, характеристики и свойства которых изменяются при функционировании (изменении режимов работы), а внешние воздействия носят случайный характер. Этап разработки математических моделей (ММ) сложных объектов управления, необходимый для решения задач их автоматизации, требует значительных интеллектуальных и финансовых затрат. Более того, большинство из них является существенно приближенными или вообще отсутствуют.В связи с этим алгоритмическое обеспечение адаптивных систем управления при реализации концепции обеспечения живучести, надежности и безопасности сложных объектов имеет ряд особенностей, включая специальные самоорганизующиеся алгоритмы автоматического формирования и периодического обновления ММ объекта и непосредственно управления.Для автоматического формирования ММ объекта предложена универсальная схема системы автоматического управления. Системы управления СТС, созданные с использованием алгоритмов оптимального оценивания, идентификации и управления объектом в штатных и аварийных режимах, являются более высококачественными по сравнению с традиционными, позволяют более обоснованно использовать контроллеры для реализации достаточно сложных алгоритмов, но не расширяют круг решаемых задач. Для реализации управления различными характеристиками (экономичностью, надёжностью, маневренностью, уровнем физических полей и т.д.) и, следовательно, обликом конкретных объектов указанные методы СТУ необходимо дополнить методами, позволяющими получить функциональные зависимости между характеристиками объекта управления и внутренними переменными в его математической модели. Такие методы должны разрабатываться совместно конструкторами, технологами и специалистами по автоматизации конкретных СТС. При наличии таких аналитических зависимостей задача оптимизации внутренних переменных объекта по различным критериям, в том числе живучести, трансформируется в задачу

оптимизации его конкретных характеристик, а система управления внутренними переменными – в систему управления характеристиками и обликом объекта. Важным и основным требованием к любой системы управления, как известно, является обеспечение устойчивости процессов. Следовательно, обеспечение и сохранение устойчивости (робастности) системой управления процессами СТС при различных неблагоприятных воздействиях гарантирует её живучесть.Возможны различные реализации адаптивных систем управления на основе приведённой структурной схемы. К числу перспективных систем, реализующих относятся системы с самоорганизующимися оптимальными регуляторами с экстраполяцией, предложенные академиком РФ. А.А. Красовским [4]. Структурная схема алгоритма самоорганизующегося управления приведена на рис.2. В этих системах сочетаются процедуры и алгоритмы оптимального оценивания параметров (идентификации) и состояния (фильтрации) управляемого процесса с алгоритмами и процедурами оптимизации управления, что приводит к построению адаптивного регулятора на принципах самоорганизации – адаптивного регулятора нового поколения. Для разработки и настройки самоорганизующихся систем не требуется знание ММ объекта, т.е. не требуется не только информация о параметрах, но и о структуре модели управляемого объекта и внешних воздействий. Использование самоорганизующихся алгоритмов управления в системах управления СТС приводит к обеспечению высокого качества и точности управления процессами на всех режимах работы сложного нестационарного объекта, а также при возникновении внешних или внутренних поражающих факторов эффективно противостоять им в связи с наличием одновременно алгоритмов структурной и параметрической адаптации, а также оптимального управления. Влияние этих факторов, связанных с изменением состояния и свойств объекта, внешних условий и нарушающих заданные технологические процессы, компенсируется автоматически этой системой до пределов, отведенных управляющим воздействиям их возникновению и, следовательно, обеспечивает его живучесть.

Туркин И.И., Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

УПРАВЛЕНИЕ ДВИЖЕНИЕМ СУДНА ПО КУРСУ С ПОВЫШЕННОЙ ЖИВУЧЕСТЬЮ

От качества и надежности системы автоматического управления движением судна по курсу – авторулевого (АР) в значительной степени зависит безопасность мореплавания, а также технико-экономические показатели эффективности эксплуатации судов. Судно, как объект системы автоматического управления движением по курсу, является сложным гидродинамическим звеном, состоящим из корпуса судна, руля и окружающей их среды. Точное математическое описание такого звена встречает большие трудности, а получаемые при этом нелинейные уравнения чрезвычайно сложны. При этом гидродинамические коэффициенты уравнений значительно изменяются с изменением скорости хода судна и его загрузки, т.е. судно является нелинейным нестационарным объектом. Поэтому на практике для синтеза систем автоматического управления движением судна по курсу используют упрощённые линейные стационарные математические модели объекта, коэффициенты которых при различных вариантах нагрузки и скоростях хода различаются на порядок и выше.

Одним из основных направлений решения этой проблемы являлось создание автономных адаптивных авторулевых, обеспечивающих в большинстве случаев автоматическую настройку параметров (параметрическую адаптацию) системы при изменении состояния объекта управления и внешних условий плавания (скорости хода, осадки судна, состояния погоды, глубины под килем). Опыт эксплуатации таких адаптивных авторулевых подтвердил повышение их технико-экономической эффективности по сравнению с традиционными авторулевыми.

Параметры модели в процессе адаптации могут оставаться неизменными, оцениваться теоретически по данным о параметрических возмущениях, идентифицироваться в режиме работы или в специальном режиме. В самонастраивающихся АР условно можно выделить системы с пассивной, активной и комбинированной адаптацией. Пассивная адаптация применяется, когда факторы, влияющие на качество регулирования, измеряемы, их можно рассчитать, как изменить параметры АР, чтобы качество управления осталось хорошим. При такой адаптации коэффициенты закона регулирования находятся по определенной программе в зависимости от результатов контроля возмущений. Для реализации пассивной адаптации необходимо предварительное исследование системы, в процессе которого должна быть установлена зависимость между коэффициентами закона регулирования и факторами, влияющими на его качество. Так как возмущения, действующие на судно, весьма разнообразны и большинство из них не поддается измерению, то область применения пассивной адаптации ограничена. Такой вид адаптации может быть использован для подстройки АР к изменению скорости хода судна, либо к изменению его загрузки.

Для сравнительного анализа оптимального самоорганизующегося авторулевого и авторулевого с ПИД-законом, их работоспособности и живучести, было выполнено имитационное моделирование их работы применительно к судну с водоизмещением 6000 т. В качестве

неблагоприятных внешних факторов рассматривались изменения эксплуатационных режимов судна по скорости и загрузке. Коэффициенты математической модели судна были определены экспериментально для трёх режимов – а) скорость 10,7 узлов, порожний; б) скорость 9,5 узлов, с грузом; в) скорость 5 узлов, с грузом. Сравнительный анализ авторулевых проводился в динамических и установившихся режимах их работы.

Для обеспечения работоспособности такого авторулевого требуется настройка коэффициентов ПИД-закона для вариантов б) и в), что и делается на практике. Самоорганизующийся авторулевой обеспечивает при всех вариантах скорости хода и загрузки судна (и одних и тех же других условиях) требуемые показатели устойчивости и качества регулирования, что свидетельствует о высокой живучести системы. Результаты моделирования показывают потенциальные возможности самоорганизующегося авторулевого, что позволяет его считать адаптивным авторулевым нового поколения.

Туркин И.И.,Алексеев А.В., Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

К ВОПРОСУ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ АВТОМАТИЗИРОВАННЫХ СУДОВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

В соответствии с одним из определений, которых сегодня не менее пяти, под живучестью понимается способность технических средств (систем) к сохранению своих основных функций (хотя бы с допустимой потерей качества их выполнения) при воздействии факторов внешней среды и неблагоприятных условий эксплуатации. Автоматизированные судовые технические средства (СТС) представляют собой комплексы, включающие непосредственно технические средства (ТС) и систему управления (СУ) ими. В связи с этим живучесть таких комплексов в значительной мере определяется не только живучестью самих ТС, так и особенностями его СУ. Важнейшими характеристиками систем автоматического управления процессами различных объектов являются количество и качество решаемых задач.

Существующие системы автоматизации СТС, как правило, разработаны на основе методов традиционной теории управления. Эти системы хорошо себя зарекомендовали при решении свойственных им простых задач (стабилизации, слежения, программного управления на основе ПИД - законов и т.д.) и являются важными в практическом отношении.

Такие системы обеспечивают управление только некоторыми выходными - технологическими переменными и, следовательно, только теми немногими характеристиками объекта, которые определяются этими переменными. Зависимость между выходными и внутренними переменными объекта обычно бывает сложной, поэтому рабочие процессы во многих элементах при определенном законе управления только некоторыми выходными переменными, по сути дела, являются неуправляемыми.

В докладе рассмотрены системные аспекты развития комплексов управления судовыми техническими средствами в условиях возникновения аварийных ситуаций и борьбы за живучесть судов. Показаны ограниченные возможности эффективного решения названных задач при использовании ряда современных структур и алгоритмов управления и в целом живучести автоматизированных судовых технических средств.

К новым, важным и неизвестным ранее задачам, решаемым на основе методов многоцелевого оптимального адаптивного управления и направленным на их совершенствование, могут быть отнесены:

—создание более экономных и надёжных конструкций объектов автоматизации за счёт расширения возможностей по формированию их характеристик с помощью различных по функциональному предназначению контуров управления;

—повышение адаптивных свойств объектов с целью максимального соответствия изменяющимся условиям среды функционирования;

—расширение областей и способов применения систем управления для повышения эффективности функционирования объектов, как в штатных условиях, так и обеспечения безопасности в аварийных ситуациях.

Сделан вывод о целесообразности перехода и возможности реализации концепции адаптивных самоорганизующихся систем управления (АССУ) применительно к условиям функционирования объектов морской техники и морской инфраструктуры. Сформулированная и рассмотренная концепция АССУ, по мнению авторов, позволяет выйти на новые уровни обеспечения живучести, надежности и безопасности автоматизированных судовых технических средств. Разработка и совершенствование специального алгоритмического обеспечения АССУ позволяет реализовывать принципы и методы самоорганизации с учетом современных возможностей и требований.

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНИЧЕСКИХ СРЕДСТВ МАССОВОГО СПРОСА

Сегодня невозможно представить человека без какого-либо технического средства массового спроса (ТСМС) типа стационарный телефон, персональный компьютер, мобильный телефон, смартфон, планшет и другие. Данные ТСМС уже глубоко вошли в нашу жизнь, поэтому безопасность при использовании данных средств должна обеспечиваться также на высоком уровне и с высшим приоритетом. Анализ рынков ТСМС показал, что они, прежде всего, развиваются с огромной скоростью. Поэтому и представляют все больший интерес для злоумышленников. В свою очередь, пользователям становится все более сложным обеспечивать безопасность собственных данных. Еще сложнее это делать пожилым людям, как менее подготовленным, для противодействия многочисленным угрозам.

В ряде представленных ниже и объединенных логически докладов в формате мастер-классе приведены практические примеры уязвимостей и технологии защиты данных применительно к основным классам ТСМС, включая ноутбуки, мобильные телефоны, смартфоны, планшеты и другие.

Как показывает анализ, имеет место известная тенденция развития ТСМС: чем больше возможностей предоставляет нам развитие техники, тем больше угроз появляется в контуре нашей собственной безопасности. Злоумышленники давно научились и непрерывно совершенствуются, используя средства нарушения конфиденциальности, доступности, целостности информационных потоков прослушивать разговоры, копировать и модифицировать фото и видео в реальном масштабе времени. Пользователи в ряде случаев настолько к этому привыкли, что не видят в этом большой проблемы. Даже подчас считают, что скрывать им даже нечего скрывать. До определенных пор это, может быть, и так. Но не учитывать то обстоятельство, что доступная для злоумышленников информация может быть весьма критичной (повлиять на жизненно важные интересы личности, общества и даже государства, как трактуется в ФЗ «О безопасности») в определенный момент времени, принципиально нельзя. Как и порох, который «всегда должен быть сухим», так и мониторинг и управление уровнем защищенности от угроз информационной безопасности (УИБ) должны быть непрерывными, эффективными и гарантированно обеспечивающими защиту жизненно важных для любого объекта безопасности информационных ресурсов.

На данном принципе, как известно, базируется социальная инженерия. Используя общедоступную или легко добываемую информацию, «информационные преступники» используют ее против своих жертв, в том числе используя факторы убеждения и доверия. И это только один из видов угроз и алгоритмов использования ТСМС.

Другим видом угроз является, например, угрозы персональной информации, хранящейся на телефоне, в том числе: номера телефонов близких и родных, которые могут быть легко подвергнуты давлению для добычи информации, шантажу, дезинформации, мошенничеству на доверии и т.п. А также - номера кредитных карт, личная переписка, электронная почта, личные фотографии, а иногда даже данные о здоровье. Фактически смартфон является «складом личной информации», которой злоумышленник может беспроблемно найти самое широкое применение в личных целях.

Планшеты хранят не меньше информации о пользователе, не исключая аналогичную информацию, а также документы коммерческого характера, включая финансовую, договорную, партнерскую информацию, в том числе оперативную и конфиденциальную.

Еще большие угрозы сопровождают использование офисной техники. Только несанкционированное подключение к принтеру или сканеру, факсу позволит злоумышленнику без труда получать копии файлов, отправленных в сеть, на ТСМС.

Не является исключением мобильная телефония. Имея специальное оборудование, можно беспроблемно прослушивать линию любого абонента. Шифрование данных также не является панацеей от этих угроз, так как дешифрирование будет производиться на уровне сотового оператора, откуда и может быть реализован съем (перехват) информации.

Одним из проверенных средств нейтрализации угроз ИБ является своевременное обновление программных продуктов и операционных систем, в которых производители «закрывают» пути обхода систем безопасности и исправляют выявленные ошибки. Очень часто пользователи пренебрегают данным фактором, что позволяет злоумышленникам также с легкостью получить необходимые данные.

Наконец, для каждого ТСМС существует угроза типа вредоносных кодов (вирусы, спам и т.п.). Один из самых опасных видов угроз, так как их инвариантность безгранична. Чаще всего оператор сам «добровольно» заражается вирусом. Сам того не подозревая, например, при установке нелицензированных программных продуктов или используя нелицензированную операционную систему.

Методы и средства борьбы с данными угрозами есть, но самое главное - оператор сам должен быть максимально мотивированным на защиту своих информационных ресурсов, персональных данных. Сегодня рынок предлагает множество сертифицированных средств защиты информации (ССЗИ) для противодействия потенциальным злоумышленникам. Но и здесь есть своя проблема: ССЗИ только в Государственном реестре ССЗИ более 3000, что проблему выбора наиболее совершенного из них превращает в «неподъемную ношу», а использовать «первое встречное» - своя «проблема рынка». Именно поэтому необходимо иметь в широком доступе доверенные данные квалиметрического представления в том числе ТСМС на рынке и их ранжирования по фактически достигаемому качеству, переход от сертификации соответствия к сертификации качества. Сегодня технологиям данного уровня (специфика рынка) уделяется совершенно недостаточное внимание. Это – известная и большая угроза.

Выполненный анализ технологий обеспечения ИБ и поддержки пользователя при использовании ТСМС показал особую актуальность сегодня системного обеспечения их развития, а также реализации комплексного подхода к обеспечению заданного уровня безопасности пользователей при использовании ТСМС с обязательной квалиметрической оценкой и сертификацией достигаемого качества ИБ, аттестацией объектов информатизации, лицензированием операторов и аккредитацией заявителей.

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРОГРАММНЫЙ КОМПЛЕКС ОБЪЕКТИВНОЙ ОЦЕНКИ КАЧЕСТВА РАЗНОРОДНЫХ ОБЪЕКТОВ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Одной из наиболее востребованных и сложных проблем сегодня в области анализа сложных организационно-технических систем, разнородных объектов информатизации и их информационной безопасности является изыскание путей повышения объективности оценки их проектного качества и достигаемой при эксплуатации эффективности. В том числе исключения или максимальной минимизации негативного влияния человеческого фактора (ЧФ) при оценивании, обеспечении его защищенности от ошибок экспертов. От достоверности получаемых при этом оценок существенно зависят последующие принимаемые обоснованные решения. Поэтому главной задачей при этом является свести к минимуму методические погрешности и погрешности оценки исходных данных.

Анализ процессов оценки качества разнородных объектов позволяет утверждать, что финальное решение далеко не всегда является объективным. Основными проблемами являются: влияние мнения коллег или иных людей на мнение эксперта; умышленное (мотивированное) завышение (или занижение) оценок по тому или иному объекту с целью собственной выгоды; отсутствие общей базы данных и её актуализация для сравнения альтернативных вариантов. Очень важным является выполнение квалиметрических оценок разнородных объектов, что в практике является далеко не редкостью. Более того, сегодня, производители часто вообще не приводят численных характеристик своих продуктов, по которым можно было бы провести сравнительный анализ. Данная проблема, тем более, актуальна для специалистов информационной безопасности, так как именно они часто встречаются с проблемой объективной оценки разнородных объектов. Например, при выборе системы безопасности предприятия, а также её элементов. Выбор наилучшего средства борьбы с угрозами является одной из важнейших задач при проектировании системы защиты информации.

С целью решения данных проблем авторами был разработан программный комплекс (ПК) многокритериального квалиметрического оценивания «МКО-ИБ» для объективно оценки качества разнородных объектов в защищенном исполнении. Ключевой особенностью данного программного комплекса является то, что он является достаточно универсальным и может быть адаптирован под любые виды оценок совершенно разнородных объектов.

ПК «МКО-ИБ» в защищенном исполнении имеет интуитивный интерфейс, который позволяет эксперту быстро и с максимальной эффективностью приступить к работе. Одной из важнейших особенностей является учет квалификации и опыта эксперта, который учитывается при оценке агрегированного показателя качества (АПК) каждого из альтернативных объектов или технологического решения.

Оценка производится на основе выставления оценок по заданным критериям в установленных границах, которые являются частными показателями качества (ЧПК). После успешного изучения материалов для экспертов и выставления индексов важности соответствующих ЧПК производится расчет групповых показателей качества (ГПК), которые агрегируются в модельные показатели качества (МПК) с учетом особенностей принятой матрицы индексов важности критериев. ГПК отражают отдельные свойства объекта или технологического решения, а МПК – его агрегированный показатель качества с учетом принятой модели оценивания. Сравнение МПК и АПК альтернативных вариантов позволяет оценить конкурентную способность объекта или технологического решения. Все

оценки и данные по экспертам шифруются симметричным алгоритмом блочного шифрования по ГОСТ 28147-89 с 256-битным ключом. Данная технология реализована с целью безопасной передачи данных администратору, а также полностью исключает угрозу модифицирования данных. Это позволяет использовать данный комплекс независимо от руководителей экспертизы, операторов и самих экспертов. По результатам использования ПК «МКО-ИБ» совет экспертов только утверждает полученные оценки и вытекающее из них экспертное решение, чем и обеспечивается информационная защита оценок от возможности субъективного влияния участников экспертизы на результаты.

ПК «МКО-ИБ» прошел к настоящему времени весь заданный объем тестирования, испытаний и использования в ряде конкретных задач, подтвердив при этом верность принятых концептуальных и технологических решений, простоту, удобство использования и защищенность от влияния ЧФ.

Тем самым, его главным подтвержденным преимуществом явилась возможность обеспечения максимальной объективности экспертного оценивания за счет принятых и представленных выше организационно-технических решений. Кроме того, данное программное решение позволяет эксперту оставаться полностью анонимным, включая результаты оценки. Полное исключение взаимодействия с другими экспертами позволит эксперту быть практически независимым (объективным) от взаимного влияния экспертов. Сегодня это решение может успешно использоваться, как при проектировании сложных объектов информатизации, так и при проведении тендеров, конкурсов и других задачах альтернативного выбора с учетом достигаемых при этом показателей качества и его агрегированной (интегральной) оценки по технологии многокритериального полимодельного оценивания.

Шаров А.И. , Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Мобильные телефоны (МТ) появились сравнительно недавно, но прочно вошли в нашу жизнь, практически являясь главным средством коммуникаций среди средств массового спроса. Мобильная телефония, обладая целым рядом неоспоримых достоинств (общение практически из любой точки пространства, высокое качество связи, целый спектр сервисов, пакетная передача данных, постоянная доступность для других пользователей и др.), тем не менее, имеют немало уязвимостей и реальных угроз, которыми могут воспользоваться злоумышленники.

В докладе в формате мастер-класса для пользователей технических средств массового спроса (ТСМС) без специальной IS-подготовки в систематизированном виде приведен типовой набор обязательных, по нашему мнению, регламентов обеспечения ИБ МТ. Для эффективной защиты соответствующих ИР продемонстрированы соответствующие технологии защиты и дан анализ качества нейтрализации соответствующих угроз.

К числу угроз, специфичных для МТ относятся: отсутствие доверия к штатным механизмам обеспечения ИБ МТ. Несанкционированное удаленное управление МТ. Несанкционированный доступ к информации, хранящейся и обрабатываемой в МТ. Несанкционированное использование интерфейсов МТ.

При этом, одной из распространенных уязвимостей МТ является также их банальная кража. Поэтому необходимо использовать соответствующие предиктивные меры защиты типа: сохранять постоянную бдительность и периодически контролировать наличие телефона; использовать наушники, что может гарантировать почти полную безопасность телефона относительно кражи, так как наушники подключены непосредственно к телефону и их отключение будет моментально замечено пользователем.

Одним из средств защиты от прослушивания является мобильное средство коммуникации (МСК). Оно предоставляет пользователям (работникам) организации возможность использования МСК, как в режиме обычного мобильного телефона (незащищенный голосовой вызов/голосовые данные), так и в защищенном режиме, с использованием наложенных средств криптографической защиты. При этом МСК обеспечивает: защиту мобильного устройства и информации, хранящейся на нем;защищенный доступ к ресурсам государственной информационной системы; конфиденциальный обмен данными.

Введение ограничений на функционал МСК включает: загрузка на МСК (и обновления) только ПО из банка доверенных приложений. Возможность блокировки экрана в соответствии с политикой ИБ (тайм-аут, пароль). Возможность блокировки USB для доступа к памяти (интерфейс можно использовать только для зарядки). Возможность отключения использования мессенджеров (входящие и исходящие сообщения). Возможность отключения использования штатных средств голосовой связи (входящие и исходящие звонки). Возможность отключения модема или оборудования с аналогичными возможностями. Возможность отключения интерфейсов: Bluetooth, Wi-Fi, камер, микрофона. Возможность отключения любых сервисов и службы геопозиционирования. Возможность блокировки

доступа к МСК после ряда ошибок при вводе пароля (в соответствии с политикой). Наличие встроенного межсетевого экрана (МЭ), сконфигурированного в соответствии с политикой ИБ. Взаимодействие МСК с системой управления КСМС: Возможность задания на МСК требований к паролям и других ограничений в соответствии с политикой ИБ. Возможность обновления политик ИБ. Передача данных о событиях на МСК. Возможность запуска/остановки приложений по командам КСМС.

Требования политики ИБ: выход в интернет с МСК только через корпоративный шлюз. Возможность дистанционного запрета на использование отдельных интерфейсов МСК. Возможность дистанционного блокирования МСК и уничтожения данных при наступлении событий ИБ. Возможность дистанционного обновления прошивки, системных приложений и сервисов МСК.

Основными направлениями обеспечения ИБ при использовании МСК в процессах обработки данных, являются: технические ограничения на функционал МСК; централизованное (дистанционное) управление настройками безопасности МСК; обеспечение требований к МСК в части технической защиты информации; контроль использования МСК.

Таким образом, возможности МСК дают определенную гарантию в том, что злоумышленникам будет создано достаточное информационное противоборство при атаках на мобильную телефонию. Безопасность использования МТ, прежде всего, зависит от самих пользователей, их заинтересованности в безопасном общении и собственной безопасности.

Вместе с тем, так как несанкционированное прослушивание мобильной телефонной линии дает злоумышленникам значительную информацию для реализации весьма большого количества традиционных и новых векторов атак, которые могут принести весьма большие потери, как для пользователя, так и компании в целом, задача гарантированного обеспечения ИБ при использовании МТ должна быть приоритетной в соответствии с ФЗ «О безопасности». Причем, прежде всего, государства (эффективные сертификация, лицензирование, аттестация объектов информатизации). Обязательно далее - общества (работодатели) И только потом - пользователей (личности). В обратном порядке – вариант, очевидно, малоэффективный. И, даже, бесперспективный.

Шитикова К.А.. Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ОФИСНОЙ ТЕХНИКИ

Офисная техника уверенно вошла в жизнь практически каждого человека. С появлением таких технических устройств, как персональный компьютер (ПК), принтеры, факсы, копировально-множительные устройства, сканеры, шредеры и др. в массовом потреблении возросла уязвимость информационных ресурсов, как отдельных пользователей, так и информационных ресурсов целых организаций. При этом массовый спрос на офисную технику не обеспечивает гарантированной защиты используемых информационных ресурсов (ИР). Более того, порождает целую группу угроз информационной безопасности (ИБ), обусловленной недостаточным уровнем подготовки широкого круга пользователей, использующих офисные средства, как технические средства массового спроса (ТСМС), в такой специфической области, как организация и технологии защиты информации. А также традиционно опережающим темпом развития технологий информационных вторжений, нарушения конфиденциальности защищаемых информационных ресурсов, их доступности, целостности и т.п.

Для обеспечения ИБ при использовании технического оборудования офиса необходимо тщательно проанализировать все возможные угрозы безопасности автоматизированной системы. Традиционно эта задача решается в ходе специально проводимых мероприятий, включая аудит ИБ. Тем не менее, это может быть и, по нашему мнению, должно быть задачей каждого пользователя. Естественно, с привлечением ответственных специалистов при необходимости.

В докладе в формате мастер-класса для пользователей ТСМС без специальной подготовки в систематизированном виде приведен типовой набор обязательных, по нашему мнению, регламентов обеспечения ИБ для эффективной защиты соответствующих ИР, продемонстрированные соответствующие технологии защиты и дан анализ качества нейтрализации соответствующих угроз.

Среди уязвимостей и угроз при использовании ТСМС (типовой регламент 1) рассматривается порядок определения и назначения (разработчиком новых ИР) степени защищенности (грифа ИР, его ранга с позиций ИБ) и необходимости соответственных регламентов, установленных в организации.

Далее рассмотрены уязвимости, обусловленные отсутствием у пользователя навыков при работе с некоторыми из многочисленных средств офисной техники. В частности, с ПК, многофункциональными устройствами, факсимильными аппаратами и др. Эта уязвимость ИБ может повлечь за собой выход из строя, как одного из устройств, так и системы в целом.

Помимо этого не стоит исключать такой вариант угроз ИБ, когда в организации «находятся» пользователи, имеющие доступ к защищаемым ИР и возможность передать некоторые из них третьим лицам, которые не имеют права доступа к этим данным.

При работе с данными ограниченного распространения, а, тем более, с секретной информацией не стоит исключать возможности доступа к ИР с помощью специальных устройств технического шпионажа. основанных на соответствующих физических принципах. Включая специальные программные средства типа средств, использующих вредоносные коды (вирусы, спам и т.п.).

Рассмотрены угрозы ИБ, обусловленные искажением или уничтожением ИР, как непосредственно нарушителями регламентов ИБ («информационными преступниками»), включая злоумышленников по признаку «преступления» установленного порядка ИБ. В том числе косвенно, например, с использованием тех же вирусных программ, а также с хищением физических носителей информации, не предназначенной по регламентам данной организации для широкого круга пользователей.

К числу уязвимостей ИБ, по нашему мнению, следует относить даже недостаточную «информационную культуры пользователей ТСМС» в части недооценки практических рисков ИБ и их последствий,связанных в том числе с несанкционированным доступом посторонних лиц к конфиденциальной информации пользователя. Оценка рисков должна производиться адекватно существующей ситуации и регулярно на каждом рабочем месте, в том числе с проведением специальных учебно-тренировочных мероприятий в достаточно широком диапазоне их возможностей.

К примеру, возможность случайной ошибки пользователя, из-за которой информационные ресурсы могут быть подвержены искажению или полному уничтожению типа: не те документы попали в шредер, или по неосторожности пользователь уронил жесткий диск с важной информацией, которую очень трудно восстановить. В ряде случаев этот риск намного выше, чем использование специальных средств съёма информации. И эти риски и ущербы важно также оценивать в каждой из возможных ситуаций, когда уровень ИБ может снизиться до угрожаемого. Бесспорно, только на основании полученных данных можно эффективно принимать необходимые практические меры по защите ИР.

Сделан вывод о необходимости обеспечения в процессе повышения надёжности защиты ИР системной целостности (комплексности) программно-аппаратных, организационных, инженерно-технических мероприятий, которые должны быть обоснованно разработаны для каждой информационной системы, включая каждого пользователя индивидуально в составе организации в целом, исходя из целей и решаемых задач организации, непременно, с учетом категорией используемых ИР.

Так, для организаций, работающих с использованием секретной информацией, как известно, необходимо выполнять предиктивные меры по защите ИР, а именно осуществлять предварительную проверку всех имеющихся средств офисной техники на наличие в них устройств несанкционированного доступа типа «закладных устройств».

Не менее важным для поддержания должной безопасности ИР пользователя является постоянный мониторинг системы их защиты, контроль действий каждого пользователя, своевременное реагирование и принятие мер при нарушении (или попытках нарушить) установленных регламентов.

Таким образом, представленные результаты анализа практики обеспечения ИБ пользователя при использовании офисной техники, как ТСМС, и предлагаемая система дополнительных мер по защите ИР пользователя) позволит, по мнению авторов, повысить эффективность работы как отдельного пользователя, так и всей автоматизированной системы в целом.

Удодова Е.Н.
Россия, Санкт-Петербург, ФГУП «Крыловский государственный научный центр»

МЕТОДИКА АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ И МОНИТОРИНГА КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЙ СУДОСТРОИТЕЛЬНОЙ ПРОМЫШЛЕННОСТИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Повышение конкурентоспособности (КС) организации – залог повышения КС страны. В понятие КС организации вкладывается ее способность выпускать конкурентоспособную на конкретном рынке продукцию, ее преимущество по отношению к другим фирмам данной отрасли внутри страны и за ее пределами. Количественная оценка и анализ КС, выявление тенденций её изменения с использованием технологий мониторинга, анализ факторов влияния на неё – все эти задачи становятся особенно актуальными в условиях решения приоритетной национальной задачи обеспечения КС и импортозамещения продукции.

Основой для оценки КС любого вида продукции должно являться комплексное исследование рынка методами прикладного системного анализа и маркетинга, что позволит не только определить некоторый «базовый образец» (лидер отрасли), но и оценить его место на данном рынке в сопоставлении с аналогичными оценками реальных и возможных объектов рынка. Оценка КС предприятия в целом – более сложная задача. Существуют определенные экономические, финансовые показатели, например прибыльность, производительность, оборачиваемость, деловая

активность, ликвидность, которые характеризуют результативность деятельности фирмы. Однако они не дают однозначного ответа о динамике КС предприятия на рынке в целом.

Для этого в методологическом плане, прежде всего, представляется целесообразным сформировать систему «прозрачных» критериев анализа, технологий оценивания, а также мониторинга (непрерывного наблюдения) состояния, как отдельных предприятий, так и отрасли машиностроения в целом. Это, в свою очередь, позволит оперативно реагировать и конструктивно управлять этими сложными процессами. Был проведен анализ критериев оценки КС, используемых различными авторами в комплекте с различными методами расчёта, который показал, что единого подхода к оценке КС предприятия не существует, так же как не существует единого алгоритма. В связи с этим предлагается использовать метод экспертного оценивания, так как оценка КС – сложная задача, использующая множество параметров, многие из которых являются качественными и трудно представляемыми количественно (измеряемыми).

Проблеме оценки КС предприятия посвящены труды широкого круга авторов, включая таких, как Азоев Г.Л., Ансофф И, Боумэн К., Винокуров В.А., Воробьёв Н.Н., Горбашко Е.А., Григорьева А.А., Григорьева А.П., Завьялов П.П., Завьялов П.С., Захарченко В.И., Зубов И.В., Маршалл А., Тащиян Г.О. и другие. В работах этих авторов встречаются разные подходы и методы определения и оценки уровня КС предприятия, но принципиально они могут быть сведены в девять основных модельных групп:основанных на анализе сравнительных преимуществ; на положениях теории равновесия фирмы и отрасли; на основе теории эффективной конкуренции; на положениях теории качества товара; на основе матричных методов оценки КС; на основе агрегирования частных показателей в интегральный; на положении теории мультипликатора; на основе определения позиции в конкуренции с точки зрения стратегического потенциала предприятия; на основе сравнении с эталоном.

При проведении представляемых исследований каждая группа методов была оценена методом экспертного оценивания с использованием десятибалльной шкалы, после чего произведено агрегирование оценок по комбинированному (аддитивно-мультипликативному) алгоритму и выполнено ранжирование полученных оценок агрегированного (сводного) показателя качества (АПК) метода. Предварительные оценки АПК показали предпочтительность методов в следующей ранжированной последовательности: 9 – 6 – 4 – 2 – 5 – 8 – 7 – 1 - 3.

Предложен авторский полимодельный метод расчета КС предприятия, основанный на экспертной оценке выбранных критериев. Данный метод учитывает не только факторы, влияющие на качество и КС продукции, но и критерии, описывающие все предприятие в целом, учитывает его ресурсную обеспеченность, эффективность производственной деятельности, рациональность управления и т.д. Расчет проводился на основе аддитивной и мультипликативной модели оценки групповых показателей качества с последующим применением гармонической модели, которая дает наиболее приемлемый и хорошо интерпретируемый результат.

На основе одного блока данных был произведен расчет предложенным полимодельным методом и наиболее высокорейтинговым сегодня методом – так называемым «методом радара». Полученные данные согласуются на уровне 10 %, но при этом авторский метод является более гибким, так как дает возможность задавать «вес» каждого из показателей качества, как частных, так и групповых. Такая гибкость модели позволяет адаптировать ее к специфике различных предприятий отрасли и, естественно, за счет этого адекватнее их сопоставлять.

На следующем этапе исследований планируется выполнить многовариантные оценки и анализ КС базовых предприятий отрасли с учетом специфики обеспечения КС всего спектра их продукции с выработкой соответствующего комплекса научно обоснованных рекомендаций.

Урубков П.И., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

ПРАКТИКА ИНФОРМАЦИОННО-ПОИСКОВОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ«АНТИПЛАГИАТ»

На данный момент в мире идёт усиление борьбы с неправомерным использованием чужой интеллектуальной собственности. Среди факторов риска - проникновение широкополосного интернета, удешевление доступа к нему, рост количества сервисов и услуг, которые можно получить удалённо, доступность систем электронной коммерции стимулируют нарушения в области авторского права.

Под плагиатом сегодня понимают умышленное присвоение авторства чужой работы или её части (заимствование чужих материалов без должных ссылок).Правовое поле ответственности за плагиат регулируется авторским и смежными правами. Немалое внимание привлекает плагиат в работах чиновников, учёных, работников высшейшколы, других лиц. Согласно мнению подавляющего большинства (согласно опросам, например, см.опрос «Левада-Центра» от августа 2013 г.), плагиаторы должны немедленно лишаться своихдолжностей и званий.

До недавнего времени борьба с плагиатом в научных работах носила эпизодический характер.Общественный резонанс получали лишь самые громкие случаи. Связано это, отчасти, с

дороговизнойпроведения лингвистической экспертизы и несовершенством нормативной базы. К настоящемувремени существуют и, не смотря на все их недостатки, активно используются системыавтоматизированной проверки на плагиат. Они способны в корне изменить ситуацию по борьбе сплагиатом в сфере образования и науки. Они упрощают начало процедуры лингвистическойэкспертизы и вынуждают совершенствовать связанные юридические процедуры.Одной из таких систем является российский интернет-проект "Антиплагиат" - программно-аппаратный комплекс проверки текстовых документов на наличие заимствований из открытых источников в сети Интернет и других источников. Проект доступен как для рядовых пользователей, так и (в специальной версии) для высших учебных заведений.

Другим интересным применением технологий «Антиплагиат» следует, по мнению авторов, считать его уникальные информационно-поисковые возможности по выявлению наиболее значимых альтернативных работ и соответствующего круга специалистов в данной предметной области. Сегодня, в условиях обилия информационных ресурсов автоматизация процесса контекстного поиска представляется весьма значимым достоинством, а технологии «Антиплагиат» этому весьма способствуют.

Согласно утверждённой Министерством образования и науки «Стратегии развития системыподготовки рабочих кадров и формирования прикладных квалификаций в Российской Федерации напериод до 2020 года» уже в ближайшее время ожидается:

1) создание базы экземпляров всех работ: квалификационных работ обучающихся, кадров высшей квалификации и современных учебников, её интеграция с ЕИС ВАК (за 2013 г.);

2) обеспечение доступа частных производителей программного обеспечения к базе контрольных экземпляров работ и их текстам. Предоставление образовательным и научным учреждениям доступа к системам контроля заимствований на любых приемлемых, в том числе коммерческих условиях. При этом право выбора соответствующих информационных систем должно остаться исключительно за самим учреждением (за 2014 г.);

3) уточнение правового (юридически значимого) определения термина «недобросовестное заимствование» (плагиат) в контексте проверки квалификационных работ;

4) создание организационно-методической базы для построения системы антиплагиата в научных и образовательных учреждениях;

5) изменение требований к промежуточной и итоговой аттестации в образовательных учреждениях. Изменение процедуры регламентированного контроля качества образования в части обязательных требований к использованию систем контроля заимствований (к 2016 г.).

Вместе с тем, с появлением централизованных баз с контрольными, курсовыми, дипломными, диссертациямисуществует следующая уязвимость (опасность) автоматизированной проверки работ на наличие плагиата. Дело в том, что работы, логично предположить, должны храниться в их оригинальном виде – в том виде, вкотором они создавались. Вероятно, это будет один из пяти самых распространённых форматов (т.н.«форматы» файлов .doc, .docx, .rtf, .pdf, .odt или специально предназначенный для архивногохранения документов формат PDF/A).

Общеизвестно, что в файлах форматов PDF (в т.ч. PDF/A), атакже DjVu хранимый текст отделён от его представления, аналогичного назначения манипуляциюможно произвести и с другими форматами. Но в них это несколько сложнее. Таким образом, непредставляет особой сложности создание соответствующих документов, имеющих разное видимое (инапечатанное) и текстовое (анализируемое) представления.

Среди решений данной проблемы предлагается обсудить вопросы:

1) проверки только отсканированных печатных работ (что существенно более ресурсоёмко и трудоёмко);

2) сдачи работ как оригинальными файлами, так и виде текста с учётом разницу между ними;

3) проверки извлекаемого текста, но программами, форсировано его извлекающими из представления документа (таких программных средств, как нам известно, пока нет).

Таким образом, анализ практик информационно-поискового использования технологий «Антиплагиат» показывает целый ряд весьма значимых проблем, которые коренным образом изменяют ситуацию по противодействию плагиату и, прежде всего, в сфере образования и науки.

Ушакова А.В.
Россия,Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

АНАЛИЗ ТЕХНОЛОГИЙ И ВОЗМОЖНОСТЕЙ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ В СУДОВЫХ СИСТЕМАХ СВЯЗИ

Парольная защита является одним из основных способов защиты информации, как в отдельных компьютерах и системах, так и в сетях мирового масштаба. Целый ряд данных, хранящийся в судовых системах связи (персональные данные, коммерческая информация, данные партнеров) носят конфиденциальный характер и вследствие этого нуждаются в надежной защите.

Слабая парольная защита приводит к возможности несанкционированного доступа к информации различного уровня критичности. Данная проблема актуальна при защите конфиденциальной информации.

Для анализа технологий и возможностей парольной защиты данных необходимо изучить не только технологии парольной защиты, но и различные методы вскрытия паролей. В настоящее время существует множество методов для определения пароля. Знание этих методов и их анализ являются основой для того, чтобы сформулировать правила парольной защиты, обеспечивающие максимально надежное противодействие попыткам несанкционированного доступа к информации.

На наш взгляд, из всех методов вскрытия паролей наиболее эффективными следует считать:

–использование программных закладок;

–удаленный доступ к компьютеру;

–перехват паролей с использованием технических средств.

Для получения паролей, хранящихся в памяти компьютера, в том числе, системных паролей могут использоваться специальные программы – программные закладки, скрытно устанавливаемые в атакуемый компьютер с целью получения информации о пользовательских паролях.

При удаленном доступе к компьютеру, получение пароля злоумышленником возможно при успешном проведении сетевых атак и получении возможности удаленного управления компьютером.

Использование технических каналов утечки для получения конфиденциальной, в том числе парольной, информации является весьма непростой, но решаемой задачей. В подавляющем большинстве случаев используются электромагнитный и электрический каналы утечки, реже – оптический канал, предполагающий возможность визуального наблюдения за процессом ввода информации. Такое наблюдение может осуществляться с использованием оптических приборов или видеокамер.

Несмотря на многообразие методов вскрытия парольной защиты, нельзя утверждать, что любой пароль можно вскрыть. Существует множество способов и технологий защиты пароля от взлома. Наиболее эффективно противодействовать несанкционированному доступу можно, сочетая парольную защиту с другими методами ограничения доступа, например, использующими биометрические технологии идентификации по отпечаткам пальцев, радужной оболочке глаза или другим индивидуальным характеристикам.

Также в защите от несанкционированного доступа важную роль играют: традиционная, но не менее эффективная организация плановой частой смены паролей; разграничение доступа и строгое соблюдение правил хранения паролей.

В докладе приведены результаты анализа различных методов вскрытия паролей и технологий парольной защиты данных, что позволяет повысить уровень защиты от несанкционированного доступа. Приведены оценки возможностей вскрытия многоразрядных паролей известными средствами. Показана особая значимость и актуальность совершенствования технологий и средств парольной защиты информационных ресурсов в судовых системах связи.

Ушакова Н.П., Москаленко В.А.
Россия, Санкт-Петербург, ОАО «Концерн «НПО «Аврора», Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

СОЗДАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ БОРЬБЕ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ

В докладе представлен анализ задач и проблем, которые необходимо решить разработчику при подготовке и разработке информационных технологий по обеспечению живучести 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 создание информационных технологий и определен путь решения, это: провести сбор, изучение и анализ информации по системам информационной поддержки, локализации аварийных ситуаций морских объектов; определить задачи, сформулировать требования к информационному, математическому и программному обеспечению и разработать решения по конструктивной и аппаратной реализации системы информационной поддержки лица принимающего решения.

Главным отличием, иерархического построения систем поддержки принятия решений, является использование методов и технологий искусственного интеллекта в качестве основных средств борьбы с неопределенностью внешней среды. Необходимость интеллектуализации каждого из уровней управления обусловлена подверженностью выполняемых ими функций влиянию различных факторов неопределенности.

Практическое воплощение этой концепции предполагает избирательное использование тех или иных технологий обработки знаний в зависимости от специфики решаемых задач, особенностей управляемого судна и борьбы за его живучесть, функционального назначения как судна (корабля) в целом, так и его технических систем, условий эксплуатации и т. д.

При проектировании, построении и программной реализации системы назначение структурных элементов и функциональных задач пользователей СППР необходима ее ориентация для поддержки принятия решений в рамках определенной предметной области или нескольких областей, а также решение различного класса управленческих задач в соответствии с этими предметными областями.

В разработанной схеме существует возможность использования баз данных и баз знаний, необходимых для хранения, мониторинга и анализа больших объемов информации для работы интеллектуальной системы, ориентированной на поддержку принятия решений различных классов задач.

Наличие комплексного набора алгоритмов, методов поддержки принятия решения, используемых на каждом этапе, позволит значительно увеличить число функциональных задач в области управленческой деятельности судоводителя (командира).

Создание технологии (информационной технологии) для разработки систем информационной поддержки руководителей при борьбе за живучесть корабля наукоемкий процесс и требует от разработчика привлекать не только программистов, но и специалистов знающих прикладную область, т. е. организацию подготовки и ведения борьбы за живучесть корабля.

Филиппова А.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет

СЕТЕВОЙ МОНИТОРИНГ БЕЗОПАСНОСТИ МОРСКИХ ОБЪЕКТОВ

В настоящее время угрозы информационной безопасности (ИБ) объектов морской техники и морской инфраструктуры (ОМТИ) становятся все более сложными. Злоумышленниками реализуются более замысловатые атаки с целью взлома различных систем и получения данных. Сетевой мониторингбезопасности (СМ) предназначен для обнаружения потенциальных угроз своим сетям на ранних стадиях, улучшения работы сетей и для постоянного наблюдения за их работой.Причем, специфическим источником добываемых данных являются не только массивы наблюдаемых данных, но, самое главное, их динамика.

Более того, именно сегодня, по мере наращивания сложности используемых сетей и объектов информатизации, все больший интерес приобретает мониторинг не частных (первичных) параметров сетей, а мониторинг их групповых, модельных и агрегированного (сводного, интегрального, системного, обобщенного и т.п.) показателей. Кроме того, не в режиме апостериорного анализа многочисленных графиков, таблиц и других аналитических данных (которые, к сожалению, сегодня приходится настраивать, либо адаптировать к специфике решаемой задачи), а в режиме «прямого» анализа в реальном масштабе времени, с возможностью прогнозирования и, обязательно, с возможностью своевременного реагирования.

В качестве инструмента СМ возможно использование сетевой системы обнаружения вторжений типа NIDS(networkintrusiondetectionsystem). Она отслеживает такие виды вредоносной деятельности, как DoS-атаки, сканирование портов и попытки проникновения в сеть. Такая система сравнивает весь входящий, исходящий и локальный трафикс заранее заданными сигнатурами атак. Как только что-то попадает под сигнатуру атаки, администратор получает уведомление о попытке вторжения.

При несвоевременном обнаружении угроз корпоративной сети, разнообразные по структуре атаки могут нанести серьезный ущерб предприятию. Как известно, основными целями хакерских атак являются захват контроля над локальной вычислительной системой, ее дестабилизация или отказ в обслуживании. В свою очередь, они могут привести к таким последствиям, как потеря доступа к критичной информации, отсутствие возможности осуществления основной деятельности и другим. В общем случае, диапазон вариантов воздействий - весьма широкий.

Как и любая система, NIDSимеет свои преимущества и недостатки. К преимуществам данной технологии можно отнести: централизованное управление;отсутствиевлияния на производительность и топологию сети; просмотр большой сети за счет оптимального расположения нескольких NIDS.

А к негативным свойствам NIDSмогут быть отнесены:высокая ресурсоемкость (у NIDSмогут возникнуть трудности при обработке всех пакетов в большой/занятой сети, поэтому имеется вероятность того, что она может пропустить распознавание атаки, которая началась при большом трафике); отсутствие возможности анализировать зашифрованную информацию; отсутствие возможности распознать результат атаки (NIDSне может определить были ли атака успешной, а может установить только факт того, что атака была начата). Это означает, что после установки факта начала атаки, администратор должен, к сожалению, вручную исследовать каждый атакованный хост для того, что выяснить, произошло ли реальное проникновение.

У NIDSимеются некоторые «перекрытия» выполняемых функций с межсетевыми экранами (МЭ). Отличием NIDSот межсетевого экрана является то, что МЭ ограничивает и контролирует только параметры сессии (IP-адреса, номера портов, состояние связей) и не отслеживает вторжения в целом, происходящие внутри сети.

NIDS,в свою очередь, анализирует передаваемые данные, пропуская их, и непосредственно сигнализирует при обнаружении подозрительной активности.

Таким образом, сетевая система обнаружения вторжений типа NIDS является только одним из средств хорошей архитектуры обеспечения безопасности сети и многоуровневой стратегии ее защиты. Для того, чтобы нейтрализовать ее негативные свойства, необходимо применять NIDSв совокупности с другими средствами обеспечения безопасности информации, т.е. в составе полнофункционального комплекса.

К большому сожалению, каждое из таких технологических решений приходится синтезировать автономно, хотя типовые проектные решения могут быть и в ряде случаев встречаются. Тем не менее, их квалиметрического сравнения на современном рынке систем защиты информации практически нет, что для заказчиков представляет значительные сложности.

Поэтому возникает актуальная потребность и системная задача создания парка типовых проектных решений по построению автоматизированных систем обработки информации в защищенном исполнении (АСЗИ) с соответствующими качественными и количественными характеристиками интеграции средств для полнофункциональной защиты информации.

В состав АСЗИ в качестве базовых должны входить следующие системные модули:1.Подсистему мониторинга и управления безопасностью (ПМУБ) с элементами поддержки принятия проектных и управленческих решений администратора ИБ и управления в составе АРМ администратора ИБ. 2.Подсистему разграничения доступа (ПРД). 3.Подсистему анализа защищенности (ПАЗ). 4.Подсистему защиты от вторжений (ПЗВ). 5.Подсистему защиты от вредоносных кодов (ПЗВК). 6.Подсистему криптографической защиты информации (ПКЗИ). 7.Подсистему контроля целостности информации (ПКЦ).

В сочетании с комплексом организационно-технических мероприятий (КОТМ) и системой менеджмента качества обеспечения безопасности информации (СМК-БИ) базовый комплекс средств ПМУБ, ПРД, ПАЗ, ПЗВ, ПЗВК, ПКЗИ, ПКЦ позволяют создать полнофункциональную АСЗИ. Её основными характеристиками свойств и возможностей следует считать комплекс показателей конфиденциальности, доступности, целостности информации, интегрируемые в агрегированный (сводный) показатель качества (АПК) АСЗИ при следующих уровнях задаваемых требований: 1.Уровень выполнения требований по ИБ (ВТ, порядка >90%). 2.Уровень угрозы невыполнения требований (НВТ, порядка >(90…95)%). 3.Уровень угрозы потери управления (УПУ, порядка <(50…60)%. 4.Уровень потери управления (ПУ, порядка<50%).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Долженкова Е.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

РОЛЬ НОВЫХ ЧЛЕНОВ ЕВРОПЕЙСКОГО СОЮЗА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА НАТО

Управление массовым сознанием, а также способность управления собственными информационными ресурсами и киберресурсами в настоящее время являются одной из немаловажных целей государств. Для доминирования на мировой арене, большими акторами мировой политики создаются механизмы управления данными ресурсами, а также механизмы защиты своего информационного и киберпространства.

В современных условиях происходит борьба за информационное пространство внутри государства, региона и союза. По причине того, что современные технологии позволяют стирать границы воздействия информации посредством сети интернет, международными акторами создаются различные программы и механизмы изучения и защиты информационного воздействия.

Информационное противоборство в современных условиях рассматривается совместно с вооруженной борьбой, политико-дипломатическим противоборством, экономической конкуренцией, межгосударственным научно-техническом соперничестве. Где объектами информационного воздействия являются высшее политическое и военное руководство, общественное мнение, информационные и телекоммуникационные системы, средства и системы связи противоборствующих государств, информационные ресурсы, средства информатизации вооружения и военной техники, информационные системы органов государственной власти, банковская и хозяйственная сферы.

Обозначим понятие «информационное превосходство», под которым понимается особая форма отношений между двумя государствами, когда одно из них совершает действие, которое оно не совершало бы в противном случае, благодаря распространению специально подготовленной информации.

Увеличение роли информации привело к увеличению роста информационных противоборств. Современные технологии позволили создать новые способы ведения военных действий. Одним из таких способов является гибридная война. Гибридная война – современный способ ведения военных действий, сочетающий в себе классические методы военных операций с партизанской войной, терроризмом, информационной (кибервойной), биологической войной. В настоящее время введены в работу различные методы информационной войны, одним из которых можно считать создание ложной информации для дезинформации общества. Это можно наблюдать не только в странах ведущих гибридную войну напрямую, но и косвенно к ним относящихся, что позволяет сформировать ложное мнение общества по тем или иным вопросам, а также сформировать сознание мирового сообщества в нужном направлении.

Информационное превосходство НАТО, в контексте с информационной и геополитической составляющей гибридных войн, достигается при участии Латвии как одной из стран Европейского Союза входящей в Североатлантический военный альянс. На территории Латвии с 2014 года начал работу Центр стратегических коммуникаций в Риге (Strategic Communication Centre of Excellence), который работает в различных направлениях, таких как общественная дипломатия, связи с общественностью, а также по направлению информационно-психологических операций.

Совет Европы сотрудничает с центром стратегических коммуникаций в Риге в целях разработки общей политики с НАТО, а также содействует работе центра, создавая виртуальную рабочую среду для привлечения международных экспертов и увеличения гибкости и доступности при современных условиях. Благодаря информационным составляющим НАТО стирает статус традиционных государственных границ, управляет восприятием ситуации, изменяет приоритеты в деятельности стратегических разведок на завоевание и удержание информационного превосходства, усложняет обнаружение начала информационной операции, затрудняет создание коалиций против агрессора. Информационные операции ведутся специализированными военными и гражданскими структурами, и включают в себя все виды информации и информационных систем.Также НАТО придерживается цели создания центров данной направленности для обучения военных и гражданских лиц.

Цели информационного превосходства НАТО достигаются путем проведения семинаров, различных программ и создания центров на территориях стран входящих в состав ЕС, а также стран, чья политика направлена на сотрудничество и вступление в ЕС.

Забарин А.В., Зимичев А.М., Мезенцев Д.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России,Санкт-Петербургский государственный университет
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА

С позиций психолого-политического подхода, информационно-психологическая безопасность гражданина означает отсутствие информационного насилия над личностью в информационном пространстве данной страны и/или вооруженность личности в борьбе с различными формами проявления этого насилия.

Возникновение информационно-психологических войн относится к глубокой древности. Но сегодня приобрело невероятный размах в связи с бурным развитием информационных технологий. Их количество со временем переросло и в новое качество, ознаменовавшись феноменом так называемой «мягкой силы» или «гибридных войн». Самая эффективная геополитическая борьба происходит сегодня не на полях сражений, а в сознании человека.

Некогда этническая культура была мощнейшим инструментом обеспечения информационно-психологической безопасности для членов этноса. Человек, живущий в этносе, был защищен от деструктивного информационно-психологического воздействия извне фетишами и табу данного этноса, его религиозной и идеологической системами. Размытие сегодня понятий «нация», «раса», «государственность» приводит к тому, что этнос превращается в полиэтническую систему, причудливо сочетающую в себе элементы различных субкультур. Эти элементы могут вступать в противоречие с ценностями национальной культуры, затруднять этническую идентификацию и порождать внутриэтнические конфликты. Государственная идеология в России, согласно конституции, оказалась и вовсе под запретом. Этот запрет создал механизм разрушения духовных ценностей этноса.

За сознаниечеловека, за его ценности и потребности сегодня происходит конкурентная борьба не только со стороны политических и религиозных систем, но и со стороны участников «рыночных джунглей». Вместо умения жить по средствам навязана жизнь потребительская, сформировано желание потреблять больше и больше, вплоть до жизни в кредит. Это открыло двери баснословным прибылям спекулятивного капитала, широко использующего коммерческие информационные манипуляции, которые загоняют человека в ловушку под лозунгом - «Ничего личного, только бизнес».

Психика современного человека оказалась удивительно беззащитна. Информационно воздействие далеко не всегда воспринимается человеком как опасность. Напротив, сначала оно вызывает самые положительные эмоции, поскольку информация является источником ориентации человека в окружающей среде.

СМИ и интернет стали на сегодняшний день ведущими средствами формирования картины мира человека. Избыточность информационных потоков реализует смысл известной формулы «максимум информации равен нулю информации». Личность и ее психология ушли на задний план. превратились в рекламную вывеску. Востребованной в условиях рыночной экономики стала лишь особь с ее набором биологических и социально-биологических инстинктов.

Собственно, манипуляции процветают на ниве культуры эгоцентризма, Поэтому необходима ориентация не на отдельную особь, а на личность. А личность начинается с эмпатии – с сопереживания другим людям, с уважения и заботы о других, с умения и желания быть полезным этносу, своей стране. Главным мерилом этноцентрической культуры всегда являлся приоритет интересов этноса над частным, эгоистическим интересом. Именно эта установка является секретом выживаемости России – «нам нужна одна победа, одна на всех, мы за ценой не постоим!» Она служит основой информационно-психологической безопасности гражданина России.

Карпович С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ТЕМАТИЧЕСКОЙ МОДЕЛИ С НЕПРЕРЫВНЫМ ВРЕМЕНЕМ ДЛЯ КОНТРОЛЯ ПУБЛИКАЦИЙ В СЕТИ ИНТЕРНЕТ

В современном информационном обществе, когда информация общедоступна, большое значение для информационно-психологической безопасности, а также для государственной безопасности в целом имеет автоматизация контроля публикаций в сети интернет.

Ежедневно СМИ распространяет огромное количество новостей. Новости про различные сферы жизнедеятельности человека, например, спорт, культура, искусство, образование и многие другие. В отношении информационно-психологической безопасности важны сразу несколько моментов:

1. Доля политических и экономических новостей,
2. Появление новых трендов в новостях.

Рост доли новостей о полите и экономике может свидетельствовать о беспокойной политической или экономической ситуации в стране, может является отражением информационной

атаки на сознание граждан. В любой ситуации для предотвращения панических настроений в обществе, службы государственной безопасности должны своевременно реагировать на подобные тенденции, а государственные служащие должны принять соответствующие меры для разъяснения ситуации населению.

Зарождение новых трендов в новостях может относится к любым существующим тематикам. Например, появление нового товара или услуги может спровоцировать волну новостей, в этом случае не требуется никакой реакции со стороны служб государственно безопасности. Но когда речь идет об инновационной разработке или научном открытии, то тут скорее всего необходимо убедится в безопасности этой разработки или открытия для государства.

Для контроля новостей на заданную тему могут быть настроены специальные системы, проверяющие наличие слов маркеров в информационных потоках. Обычно составляют тематические словники, включающие все или большую часть специфических для конкретной области слов. Например, для космической сферы это могут быть следующие слова: космонавт, космос, ракета, орбита, земля, околоземное пространство, и другие. Но что делать, когда нет словаря предметной области, и не известно точно в какой тематике следует контролировать публикации? В таком случае могут помочь алгоритмы вероятностного тематического моделирования, которые на основе вероятности совместной встречаемости отдельных слов кластеризуют новости.

Тематическое моделирование — это построение модели коллекции документов, в которой определены вероятности отнесения каждого документа к теме и определены вероятности распределения слов по темам. Тематическое моделирование – это относительно молодая область исследований в теории самообучения. За последнее десятилетие было предложено большое количество различных расширений для алгоритмов тематического моделирования, были разработаны специализированные модели, учитывающие дополнительные параметры систем. В 2006 году Xuerui Wang и Andrew McCallum в работе «Topic sover Time: A Non-Markov Continuous Time Model of Topical Trends» предложили временную тематическую модель. При построении временной тематической модели наряду со стандартными распределениями слов по темам и тем по документам оцениваются распределения каждой темы по времени, что позволяет проследить и отобразить динамику изменения тем во времени.

Тематическое моделирование имеет ряд преимуществ в сравнении с другими алгоритмами автоматической обработки текстов:

1. Тематическое моделирование рассчитано для работы с большими объемами данных,
2. Для тематического моделирования не нужны словари по тематикам,
3. Для тематического моделирования не нужны размеченные данные, это самообучающийся алгоритм,
4. Тематическое моделирование будет группировать документы на основании их вероятностных оценок, а не мнений экспертов,
5. В тематическом моделировании легко могут быть учтены вероятности от других параметров исследуемой системы,т.к. результат тематического моделирования — это матрица вероятностей,
6. Результаты тематического моделирования временных моделей, наглядно визуализируются, дают представление о появлении новой группы новостей и сокращению количества новостей по отдельным тематикам.

Тематическое моделирование и в частности тематические модели во времени имеют большие перспективы для использования в различных направлениях жизнедеятельности, в том числе применимы для нужд государственной и информационно-психологической безопасности.

Кефели И.Ф.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

«ШЕСТОЕ ИЗМЕРЕНИЕ» ГЛОБАЛЬНОЙ ВОЙНЫ И ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

Пятым измерением войны специалисты называют киберпространство как ключевое звено гибридной войны (hybrid warfare), одно из определений которой звучит так: это «использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, использующих дипломатические возможности; масштабные и стремительные информационные, электронные и кибероперации; прикрытие и сокрытие военных и разведывательных действий; в сочетании с экономическим давлением» [The Military Balance 2015. The annual assessment of global military capabilities and defence economics. P. 6]. Ф. Хоффман отмечает собственно цивилизационный и геополитический характер гибридной войны как череды конфликтов, в которых противник способен применять одновременно все формы ведения войны, соединяя их «для удовлетворения собственных стратегических культурных и географических целей» [Хоффман Ф. Г. Гибридные угрозы: переосмысление изменяющегося характера современных конфликтов // Геополитика. Информационно-аналитическое издание. Выпуск XXI, 2013. – 162 стр. С. 45-62].

Начало XXI века ознаменовалось растущей интенсивностью кибератак и их выходом за пределы сферы ведения разведывательной деятельности. Киберпространство становится доступным для ведения боевых действий – наравне с землей, морем, воздухом и космосом [Department of Defense Strategy for Operating in Cyberspace. July 2011 / US Department of Defense. – http://www.defense.gov/news/d20110714cyber.pdf]. Киберпространство – пятое измерение войн глобального масштаба – заключает в себе предпосылки как информационных боевых операций, так и информационной безопасности, которые «опредмечиваются»: a) в технико-технологических и организационных средствах ее обеспечения; b) в инновационном тренде расширения пространства ведения боевых действий; c) в национальных военных и оборонных доктринах и стратегиях. Кибервойна (точнее, операции в киберпространстве, проводимые в ходе войны, а в мирное время – это диверсии, теракты, идеологическая обработка гражданского населения) является одним из магистральных направлений революции в военном деле, приведшим к появлению гибридных войн (их еще называют многомерными нелинейными войнами).

Современное и перспективное кибероружие, используемое в гибридных войнах, подразделяется на пять основных групп:

– сетевое кибероружие, обеспечивающее доступ многофункциональных компьютерных программ в закрытые внутренние военные и гражданские сети противника, включающие критические объекты.

– коммуникационное кибероружие, которое представляет собой программный код, искажающий, блокирующий и подменяющий обмен сигналами между удаленным оператором и боевым роботом.

– предустановленное кибероружие, в элементную базу которого производителем закладывается управляющий софт с различного рода «логическими бомбами», способными выводить из строя кибероружие под воздействием внешних сигналов.

– проникающее кибероружие, базирующееся на целенаправленном изменении акустической, оптической и других сред, которое приводит к модификации сигналов, поступающих на внешние сенсорные датчики высокотехнологичных вооружений и приводящих к их выходу из строя.

– электромагнитное оружие, полностью выводящее из строя в ходе превентивного удара боевую технику, «выжигая» кремниевую элементную базу наступательного вооружения противника [Е. Ларина, В.Овчинский. Пятое измерение войны http://topwar.ru/36839-pyatoe-izmerenie-voyny.html 04.12.2013].

С полным основанием следует заявить о «шестом измерении» глобальной войны и глобальной безопасности в формате информационно-психологической войны и информационно-психологической безопасности. Если первые пять «измерений» определяют объектную сторону военной деятельности в различных физических средах окружающего мира, то «шестое измерение» охватывает внутренний мир человека, его инстинкты, психику, чувства, эмоции, мысли, индивидуальное и общественное сознание. В гибридных войнах, с одной стороны, в полной мере используются организационные методы, технологии и средства информационно-психологического воздействия на личный состав и гражданское население противника, а с другой, – информационно-психологические операции армии «сильных мира сего» нацелены на то, чтобы «дать урок» превосходства своих ценностей, силы, аппетитов всему остальному миру. Эти «уроки» буквально «вываливаются» на нас из всех СМИ. Недаром бывший министр обороны США Р. Гейтс как-то «изящно» заявил по поводу утверждения принципа глобального господства Америки: «Соединенные Штаты не могут позволить себе роскошь отказа от участия в конфликтах, потому что эти сценарии не соответствуют предпочтительным для Америки понятиям о войне».

Мы явно или неявно переживаем все детали информационно-психологических операций в реальном масштабе времени и только спустя какое-то время начинаем осмысливать их геополитические и социальные последствия. По прошествии многих лет люди начинают понимать, что прежнее их восприятие текущих событий было ложным, но изменить последствия этого уже невозможно («Но время шло, и старилось, и глохло», писал Б. Пастернак).Средства и технологии информационно-психологической войны, действующие и в мирное время, способны нанести противнику не меньший ущерб, чем средства вооруженного нападения, а информационное оружие, построенное на базе технологий психологического воздействия, обладает значительно большей поражающей, проникающей и избирательной способностью.

«Шестое измерение» глобальной войны и глобальной безопасности следует анализировать, по крайней мере, в двух аспектах – геополитическом и цивилизационном. В рамках глобальной геополитики информационно-психологическая война и информационно-психологическая безопасность предстают как две грани захватившего информационное пространство геополитического противоборства, для которого, как писал еще в 1964 г. Г. Маклюэн, «земной шар теперь – не более чем деревня» [Маклюэн Г. М. Понимание Медиа: Внешние расширения человека. М.; Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. – 464 с. С. 6.]. Для цивилизационного подхода информационно-психологическая война и информационно-психологическая безопасность представляют интерес в той мере, в какой акторы цивилизационного противоборства смогут

предложить символический капитал культуры, выражающий образ национальной или наднациональной (цивилизационной) идеи, которая для большинства остается более значимой, нежели любые информационные воздействия извне.

Кефели И.Ф., Меркулов А.Л.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ГЛАВНАЯ ПРИЧИНА РАСПАДА СССР

Быстрее всех поняли значение и возможности информационных технологий американские политтехнологи. Пожалуй, можно сказать, что в организованной Западом информационной войне внедрение новейших информационных технологий имело решающее значение.

С приходом к власти в США Р. Рейгана информационное давление на СССР усилилось, еще шире стали использоваться самые новейшие информационные технологии (спутниковое телевидение, Интернет и т.д.). Появился механизм глобального скоординированного информационно-психологического воздействия на руководство и население СССР. Сегодня многими специалистами признается, что главной причиной распада СССР является его поражение в холодной и информационной войне.

Наверное, нам трудно сейчас осознать в полной мере случившуюся с нашей страной грандиозную катастрофу. Экономически мощная огромная страна с сильнейшим военным потенциалом распалась исторически мгновенно. У меня такое ощущение, что главная причина еще не названа. Меня этот вопрос заинтересовал. Конечно, мой уровень не позволяет решить эту задачу более-менее основательно, но она меня волнует, и я все же попытаюсь сделать какие-то выводы. Они, естественно, могут оказаться дилетантскими, недостаточно доказательными, научно-необоснованными, но, однако, я все же попытаюсь на своем уровне выразить отношение к этой важной теме.

Я подумал, что нелишне будет посмотреть и сравнить фазы развития социалистического строя с классическим построением стихийного (эволюционного) природного порядка. Это, во-первых. А во-вторых, трудно поверить и невозможно допустить безраздельного господства человека над природой. Это привело бы к всемирной катастрофе.

Краткий анализ по сравнительным позициям дал следующие выводы.

1. Постоянные войны, повышенная активность и напряженность в государстве, продуктивная трудовая деятельность создают и держат высокий пассионарный фон в обществе и наоборот, «головокружение от успехов», «чувство глубокого удовлетворения» внушают людям ложную безопасность, застой в развитии, распад морали и нравов.
2. Могучая Римская империя развивалась уверенно и гармонично, не имея сильных внешних препятствий. СССР появился в мире развитого капитализма, еще далекого от периода упадка; он появился во враждебном окружении, и вопрос о его падении был вопросом открытым.
3. Военная борьба за власть приводит наверх великих стратегов, мирная – посредственностей.
4. Государство, неспособное создать и содержать сильную, современную армию и флот – обреченное государство.
5. Сильное государство притягивает и объединяет народы.
6. В периоды распада империй и государств ослабляются и разлагаются все сферы деятельности.
7. Значение религии на общественное развитие зависит от многих обстоятельств. В одном случае она поднимает общество, в другом – опускает.

И когда я совместил оба графика, получилась удивительная картина. На большой, горизонтальной восьмисотлетней площади графика Римской империи я увидел высокий вертикальный штык с основанием в 70 лет.То есть явление социализма было заметным отклонением от действовавшей в данное время некой нормы эволюции, пробным показом возможного будущего человечества. Иначе говоря, это явление новой, социалистической формации было явлением преждевременным!

Так, гдеже у нас быть устойчивому развитию, когда мы сами не ведаем, что творим, а сотворив, безответственно и безоглядно запускаем в жизнь, а если и ведаем, то в большей части на пользу сильных мира.

Киряхин Н.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Ежедневно человек получает огромный поток различной информации, поступающей к нему из различных источников. Каждый день мы используем интернет, смотрим телевизор, слушаем радио, читаем печатные издания. Наш мозг принимает самые различные данные: интересные и

совершенно ненужные, вызывающие радость и заставляющие переживать за себя и своих близких. Многие из нас не способны самостоятельно справиться с таким большим количеством сведений.

Ни для кого не секрет, что люди очень сильно изменились с появлением интернета и компьютера. Психологи наблюдают резкое ухудшение умственной и эмоциональной активности человека. Зависимость от компьютера - частый диагноз в наше время. Человек проводит в виртуальном мире большую часть своего времени. Бессонница, ухудшение реакции, плохое зрение - всё это последствия «виртуальной жизни».

Информационно-психологическая безопасность личности - это некий барьер, защищающий психику и сознание человека от вредоносных информационных влияний.

Существуют различные способы психологической защиты. Они направлены на предотвращение отрицательного воздействия информации, получаемой человеком в разных ситуациях (СМИ, массовые собрания, личный контакт с кем-либо).

1-й способ защиты: «Уход» - увеличение дистанции, разрыв контакта, отдаление за досягаемую зону воздействия информации. Действия в различных ситуациях могут быть такими:

– Игнорирование определенных групп СМИ (телевидение, Интернет и пр.),
– отказ от просматривания некоторых теле-радиопрограмм, чтения газет, статей, и пр.
– Обход негативных тем во время разговора.

2-й Способ защиты: «Блокировка» - контроль принимаемой информации, использование психологической блокировки и ограждение психики. Действия:

– Отсев поступающей информации
– Эмоциональный контроль.
– Расширение зоны комфорта.
– Переход на другие темы.

3-й Способ защиты: «Управление» - контролирование источника информации.Действия:

– Контактирование с источником, участие в опросах и т.д.
– Выражение своей точки зрения.
– Применение при беседе попыток наладить хорошие, дружественные отношения

4-й Способ защиты: «Затаивание» - Управление реакцией на поступающую информацию. Выполняемые действия:

– Игнорирование действий и поступков, возникающих при определенном информационном воздействии (например, отсутствие реакции на «рекламный мусор», такой как реклама «купи немедленно» «тебе это нужно», «у всех уже есть»).
– Маскировка эмоций, и др.

Способность человека использовать различные методы психологической защиты от поступающих вредоносных данных в конце концов обеспечит ему защиту информационно-психологическую безопасностьличности.

Колотов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

А. ДАЛЛЕС О МЕТОДАХ ВЕДЕНИЯ ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ И СОВРЕМЕННОЕ СОСТОЯНИЕ БИТВЫ «ЗА УМЫ И СЕРДЦА»

Технологии ведения психологической войны тема настолько тонкая, что обнаружить следы их реального применения не просто. Отдельно стоит выделить проблему доказательности использования спецсредств и психотехнологий поскольку в ряде случаев обнаружить следы их воздействия на человека не поможет даже вскрытие. Однако некоторые признаки использования психотехнологий вполне возможно обнаружить в поведении людей, подвергшихся специальной обработке.

В данном контексте особого внимания заслуживает рассекреченный 5 мая 2003 г. доклад экс-директора ЦРУ Аллена Даллеса (1893-1969) «Brain warfare», который был сделан 10 апреля 1953 г. В данном документе на официальном уровне был дан важный обзор состояния борьбы на невидимом фронте того времени, где осмысленно применяются весьма специфические методики воздействия на психику. Аллен Даллес определил «битву за человеческое сознание» как «войну идеологий». В рассматриваемом источнике на неполных 13 машинописных страницах четко определены основные параметры войны нового типа: «Мишенью этой войны является человеческое сознание на групповом и индивидуальном уровнях. Цель состоит в том, чтобы привести сознание в состояние, когда оно больше не реагирует на свободную волю или рациональную основу, а отвечает на импульсы, внедренные извне» (Dulles A. Brain Warfare, speech to the National Alumni Conference of the Graduate Council of Princeton University, Hot Springs, VA, April 10, 1953. P. 1.).

Содержащийся в докладе призыв к ЦРУ обратить особое внимание на развитие психотехнологий был выполнен на высоком профессиональном уровне. Современное состояние «умов и сердец» населения подвергшихся соответствующей обработке ряда стран представляет серьезную угрозу национальной безопасности РФ и вынуждает обратить на эту проблему самое пристальное внимание.

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 (Ф. Ратцель), 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.

Левкин И.М., Левкин Е.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОДИКА ВЫЧИСЛЕНИЯ ИНДЕКСА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

В условиях активно развивающегося информационного обществаважнейшим элементом национальной безопасности становится информационно-психологическая безопасность (ИПБ).Специфика информационно-психологических действий заключается в том, что: во-первых, они осуществляются непрерывно; во-вторых, они осуществляются как в открытом виде (деятельность средств массовой информации, неправительственных коммерческих организаций и т.п.), так и в скрытом виде (нейролингвистическое программирование, подкуп, шантаж, запугивание и т.п.). Уровень ИПБ зависит от интенсивности и направленности информационно-психологического воздействия на население страны в целом, отдельные социальные группы, высший политический, военный, экономический и т.п. менеджмент и конкретных общественно-политических лидеров. В настоящее время в методики, позволяющей получить численную оценку этого уровня, не существует, что снижает качество процесса мониторинга информационно-психологической устойчивости страны.

В основу предлагаемой методики вычисления индекса ИПБ положен подход, разработанный ПИР-центром совместно с издательским домом Коммерсант в отношении определения индекса международной безопасности iSi.

В соответствии с этим подходом в структуре индекса информационной безопасности выделены четыре составные части, определяющих информационно-психологическую безопасность различных групп населения: глобальный уровень, (президент, премьер-министр, председатели палат Федерального собрания РФ), федеральный уровень (министры, руководители субъектов федерации, руководители парламентских партий); элитарный уровень(интеллектуальная, политическая, деловая элиты) и общественный уровень (пенсионеры, наемные работники, учащиеся, предприниматели и менеджеры.

Значение ИПБ предлагается определять путем суммирования математических ожиданий случайных величин, характеризующих степень возникновения угроз, связанных с информационно-психологическим воздействием на представителей каждой из выделенных групп с учетом соответствующих коэффициентов важности.

К числу учитываемых случайных величин предлагается отнести степень формирования таких угроз как: превращение представителей различных групп в так называемых “агентов влияния”, усиление негативного влияния деятельности негосударственных коммерческих организаций на общественно-политическую жизнь страны и ее регионов, использование концепциях в экономического развития страны сомнительных экономических теорий; политизирование справедливого негативного отношения людей на некачественные управленческие решения различного уровня; отъезд за рубеж наиболее квалифицированных специалистов; снижение уровня образования; искажение истории страны и т.п. Вероятность возникновения и развития каждой из угроз должна определяться по совокупности информационных признаков, проявляющихся в текущий момент времени. Для этого должны быть разработаны соответствующие априорные словари таких признаков, статические и динамические информационно-признаковые модели информационно-психологических угроз различной природы.

Методика вычисления индекса ИПБ будет представлять из себя следующую последовательность действий: на первом этапе – формирование типового перечня информационно-психологических угроз, их информационных признаков и построение информационно-признаковых моделей; определение путем экспертного опроса коэффициентов важности каждой группы угроз и градаций уровней ИПБ; расчет базовых значений ИПБ; на втором этапе - мониторинг информационного пространства с целью выявления информационных признаков мероприятий информационно-признакового воздействия на различные группы населения; определение по проявившейся совокупности информационных признаков вероятности наступления соответствующей информационно-психологической угрозы; непосредственный расчет ИПБ; сравнение текущего показателя с принятыми значениями градаций ИПБ.

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

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОГРАММИСТА ПРИ РАБОТЕ С СОВРЕМЕННЫМИ ИНТЕГРИРОВАННЫМИ СРЕДАМИ РАЗРАБОТКИ (IDE)

Информационно-психологическая безопасность является важной проблемой современного общества, поскольку человек ежедневно вынужден обрабатывать огромное количество информации, получаемой из различных источников (Интернет, телевидение, радио). Переизбыток информации может привести к различным формам психологических расстройств (депрессия, неврозы, страхи, фобии, апатия, интернет-зависимость). При этом проблема информационно-психологической

безопасности усугубляется массовой компьютеризацией общества. Наиболее негативному воздействию данного явления подвержены программисты, так как они вынуждены использовать интегрированные среды разработки (IDE) в течение всего рабочего дня.

Постоянное взаимодействие с IDE характеризуется утомляемостью, монотонностью труда, напряженностью, повышенной концентрацией внимания. Ежедневная подверженность вышеперечисленным воздействиям влечет за собой возникновение депрессий, синдрома хронической усталости и иных психологических расстройств. Следовательно, обеспечение эргономичности среды программирования является важной задачей для сохранения психологического здоровья программиста.

В данной работе проведен сравнительный анализ IDE, которые используются во многих компаниях, специализирующихся в сфере создания программного обеспечения. Целью исследования является определение влияния IDE на психологическое состояние индивида. Для этого исследования использованы следующие программные продукты:

- Eclipse IDE fo Java EE Developers;
- Microsoft Visual Studio 2015;
- Qt Creator IDE 3.4.2;
- Intellij IDEA 14.1.

Сравнительный анализ проводился при помощи метода экспертных оценок. Группе программистов за ограниченный промежуток времени было предложено выполнить набор тестовых заданий по оценке интерфейсов. После этого испытуемым предоставлена анкета, содержащая вопросы относительно удобства, удовлетворенности, напряженности, утомляемости во время работы с каждой из IDE. Представленные выше критерии позволяют оценить психологическое состояние испытуемых.

По результатам исследования выявлены недостатки современных IDE с точки зрения психологической безопасности программистов, а также предложены некоторые рекомендации по возможному улучшению IDE.

Выбор оптимальной IDE позволит снизить психологическое напряжение и увеличить работоспособность программиста.

Москвин С.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

СИСТЕМА ИНФОРМАЦИОННЫХ ПАРАДОКСОВ И ЕЕ ПРИМЕНЕНИЕ В ПАРИРОВАНИИ УГРОЗ ГИБРИДНОЙ ХОЛОДНОЙ ВОЙНЫ

Обострение международной обстановки, связанное с событиями на Украине, африканском и европейском континентах, а также стимулируемая деятельность, так называемых, «иностранных агентов» внутри страны, требует четкой идентификации угроз в информационно-психологической сфере. Эта задача невыполнима без четкого понимания и использования объективной системы информационных парадоксов.

Система информационных парадоксов включает в себя восемь фундаментальных неочевидных закономерностей получения, обработки и использования информации. Под информацией в данном случае понимается мера устранения неопределенности о текущих явлениях, процессах, тенденциями т.д., позволяющая четко идентифицировать угрозы первого, второго и третьего порядка значимости. Это необходимо учитывать в деятельности не только стратегического звена управления страны, корпораций, организаций, силовых ведомств, но и на уровне конкретного эксперта, ученого, потребителя информации.

Искусно подготовленная дезинформация, модифицирование информации в процессе коммуникации, использование современных психотехнологий и достижений психотроники жестко ограничивает ресурс конкурентоспособности конкретного субъекта. Примеры Ливии, Ирака, Сирии, Украины, Грузии, а также мировой экономический кризис показывают незнание, неумение или отсутствием желания овладеть технологиями использования системы информационных парадоксов.

Нурышев Г.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет

ИНФОРМАЦИОННАЯ ГЕОПОЛИТИКА: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ

Информационные технологии сегодня относятся к «оружию» огромного стратегического значения. Не случайно, информация, информационные технологии, как показывают современные геополитические процессы, стали активно понижать и вытеснять значимость таких стратегических ресурсов, как территория, природные и демографические ресурсы. Информационное пространство приобрело качественно новые измерения и стало составной частью современного геополитического пространства, что обусловливает сегодня выделение информационной геополитики в самостоятельное направление геополитической науки. Субъектами геополитических отношений в

информационной геополитике стали средства массовой информации и массовой коммуникации, медиа-холдинги, транснациональные корпорации-провайдеры, виртуальные социальные сообщества и коалиции. В этих условиях под геополитической конкуренцией понимается соперничество между геополитическими субъектами за влияние на то или иное информационное пространство, не ограничиваемое государственными границами. Асимметричный характер такой конкуренции создает необходимость определения новых геополитических приоритетов конкурентной борьбы и изменения структуры предметного поля геополитики.

В информационном пространстве различные субъекты геополитических отношений одновременно могут быть союзниками и конкурентами (противниками). Условия и закономерности геополитической конкуренции формируют цели, задачи и всю структуру информационно-психологической войны. Информационная экспансия в глобальном информационном пространстве в настоящее время поставила на повестку дня вопрос об информационном империализме, значительно опережающем по своим масштабам экономический империализм. Информационно-психологический неоколониализм является агрессивной концепцией достижения геополитического превосходства в глобальном информационно-психологическом пространстве. Поэтому одной из важнейших задач государственной системы информационного противоборства в современных условиях является противодействие стремлению агрессивно настроенных участников противоборства превратить государство в информационную колонию – сырьевой придаток, источник извлечения (выкачивания) информационных ресурсов для национальных экономик государств – лидеров информационно-психологической борьбы.

Пилькевич С.В., Еремеев М.А., Мажников П.В.
Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ГРУПП ПОЛЬЗОВАТЕЛЕЙ СОВРЕМЕННЫХ СРЕДСТВ МАССОВОЙ КОММУНИКАЦИИ В РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Процессы принятия социально-психологическими объектами решений по выбору тех или иных альтернатив, изменению оценочных отношений, трансформации взглядов и т.д. являются предметом исследований в большинстве своем гуманитарных дисциплин. Наряду с этим, всесторонняя информатизация современного общества, внедрение информационно-телекоммуникационных систем и средств массовой коммуникации, развитие кибернетики обусловило расширение перечня задач, решаемых относительно социально-психологических объектов с позиций технических наук:

– выявление реакции населения на информационные поводы, связанные с нестандартными ситуациями или значимыми общественными обсуждениями;

– мониторинг и анализ реакции общества на политические инициативы, резонансные события, публичные выступления или высказывания, пресс-конференции и т.п.;

– мониторинг общественного мнения о деятельности организации и политических лидеров;

– анализ восприятия пользователями маркетинговых, рекламных и PR-кампаний;

– расчет уровня благоприятствования морально - психологической обстановки в регионах;

– оценивание морально - психологического состояния воинских формирований силовых министерств и ведомств.

Таким образом, особую актуальность приобретает разработка модели поведения групп пользователей современных средств массовой коммуникации.

В основу разработки обозначенного класса моделей целесообразно поместить эвристики — простые и эффективные стратегии мышления, которые позволяют моделировать нерациональные процессы принятия человеком решений в различных ситуациях, выбор им доступных альтернатив.

Многочисленные исследования психологов убедительно доказывают существование конечного множества различных схем поведения, которым, в большинстве случаев, следуют люди, попавшие в типовые обстоятельства (эффекты «Золушки», всеобщего внимания, ложной уникальности, ложного консенсуса, дезинформации, синдром Дженовезе, схемы оказания помощи на основе эгоизма или альтруизма, механизмы социального влияния - конформизм, влияние группы и др.).

Поведенческие особенности социума зачастую обусловлены национальной культурной средой которая, безусловно влияет на людей, предписывая им исполнение определенных ролей. В социальной психологии известен феномен, суть которого заключается в том, что человек, исполняющий ту или иную роль, нередко усваивает сопряженное с ней поведение.

Учитывая вышеизложенное, представляется оправданным при моделировании процессов принятия социально-психологическими объектами решений по выбору тех или иных альтернатив учитывать окружающую их культурную среду.

Наиболее подходящим концептуальным объектом памяти, обеспечивающим формализацию знаний экспертов об эвристиках, национальных, религиозных и культурных особенностях исследуемых социальных групп является фрейм. Фреймовая модель представления знаний наиболее подходит в качестве формального построения онтологии, поскольку позволяет в рамках стандартной

модели описать все многообразие знаний экспертов как о сценариях взаимодействия социальных групп, так и о существенных элементах Реального Мира (культурной среды). Источниками подобной информации могут выступать автоматизированные информационно-поисковые системы, а в случае ее слабой формализации - эксперты.

Результаты научных исследований социальных психологов дают основание считать саму ситуацию в которой индивидом (и/или группой людей) осуществляется процедура выбора её неотъемлемым параметром, или иначе - контекстом. Основываясь на свойстве семантической сети располагать всю точно известную информацию о той или иной концепции в базе знаний вокруг соответствующей вершины представляется более рациональным интерпретировать контекст как множество концептов семантической сети, расположенных в некоторой окрестности от анализируемого концепта.

Кроме того, разрабатываемый подход к моделированию поведения социально-психологических объектов должен реализовать концепцию рефлексивного управления в терминах В. Лефевра, что достигается за счет своеобразного триединого рассмотрения проблемной ситуации: с позиции источника возмущающего воздействия, с позиции адресата и с позиции социальной среды (стороннего наблюдателя фрагмента реальности, в котором происходит воздействие). Что в свою очередь находит отражение в применении механизма фреймов как своеобразных сложных узлов – элементов онтологии.

Плебанек О.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Современный этап человеческой истории имеет две важные особенности, давно обсуждаемые научным и политическим сообществом: глобализация социокультурных процессов и высокая степень технической оснащенности человечества. И та, и другая стороны современного социального бытия находятся в центре исследовательского внимания представителей различных научных специальностей, но особенность научного дискурса – его дисциплинарный, поаспектный характер зачастую не позволяет увидеть проблемы и их возможные решения в объеме. В связи с этим, практически на наших глазах и нашими усилиями рождается новая отрасль научного знания – глобалистика, призванная дать комплексный подход к решению сложных проблем. Не вызывает сомнений, что коллективная безопасность является сложнейшей проблемой, не решаемой ни в рамках технической оснащенности, ни в пределах политико-правовых механизмов и институтов.

Несмотря на то, что уже несколько десятилетий существует и само понятие глобальных процессов, и сформировался целый блок исследовательских подходов в их рассмотрении, издаются монографии и довольно многочисленные журналы, все же методология глобалистики находится в стадии становления. Основной принцип глобальных исследований – комплексный подход, является необходимым, но недостаточным условием познания столь сложных процессов. Комплексный подход предполагает привлечение к исследованию объекта представителей различных научных специальностей. Такая стратегия научного исследования формировалась в русле неклассической научной парадигмы, и когда-то представляла собой новое слово в науке. В настоящее время трудно представить себе какую-либо проблему, начиная от промышленного производства и заканчивая медицинскими и политическими исследованиями, где не привлекались бы представители различных областей знания. Но современный уровень проблем, стоящих перед человечеством, требует не только комплексного подхода, но и системных исследований. Проблемы коллективной безопасности, несмотря на привлечение специалистов технического знания, информационных технологий, политтехнологий, до сих пор далеки от разрешения.

Системные исследования начали формироваться еще в середине прошлого века, понятие системы достаточно часто встречается в научной литературе, но чтение этих текстов заставляет признать, что принцип системности еще не стал базовым принципом научных исследований. Если комплексность предполагает исследование объекта методами разных научных дисциплин, то системность предполагает формирование специфического метода, направленного не на аспекты бытия объекта, а на связи, возникающие между этими различными аспектами. Эти взаимодействия трудноуловимы, характер этих взаимодействия неочевиден, ненаблюдаем в режиме on-line (не дан нам в прямом наблюдении), но решающее значение в функционировании сложных объектов имеют именно непрямые воздействия и взаимодействия элементов системы. Особенно наглядно системный характер функционирования сложных объектов проявляется в эффекте резонанса слабых взаимодействий, который совершенно меняет картину прямых воздействий. Поэтому в прикладном аспекте, обеспечение коллективной, а также государственной безопасности возможно только на пути формирования и совершенствования системных методов исследования.

Самым сложным аспектом исследования проблем коллективной безопасности, как становится ясно в связи с последними событиями, является социокультурный аспект. Современная политическая реальность нам дает обильные свидетельства того, что ни эффективный экономический базис, ни мощная военная оснащенность, ни благоприятный пространственный фактор (протяженность границ, удаленность от возможного агрессора и т.д.), ни даже в совокупности эти факторы не дают гарантий обеспечения безопасности общественной системы. Советский Союз обладал мощнейшим экономическим, военно-политическим потенциалом, но не смог обеспечить не только коллективную, но даже собственную безопасность. Можно было бы рассматривать его распад как позитивный результат социально-политических процессов (например, получение независимости национальных республик) если бы не кровавые социальные катаклизмы, обрушившиеся на население, и не глубокие экономические потрясения, спровоцировавшие эмиграцию в более спокойные геополитические регионы. Из этих потрясений мы вместе выходим с разной степенью успешности уже около трех десятков лет, и никакому новому государству нет гарантий целостности границ, экономической стабильности, обеспечения права на жизнь и здоровья граждан. Вместе с тем, сегодня совершенно ясно, что Советский Союз не был обречен историей (как не была обречена на распад Югославия), его распад был спровоцирован и режиссирован третьими действующими акторами. Оказалось, что полем для чужих игр, угрожающих независимости страны и физической безопасности ее граждан, может стать даже мощное государство с солидным военным и технологическим потенциалом (такое как Франция, Германия, государства Ближнего Востока). Оказалось, что для разрушения государственности, как показывает современная история, совершенно необязательно военное вмешательство и военные затраты, но без психологической подготовки граждан этой страны ее разрушение невозможно. Поэтому никакой проект коллективной безопасности не может быть успешным, если не содержит мероприятия и институты, обеспечивающие идеологическую безопасность.

Современная история в достаточной степени демонстрирует зависимость безопасности взаимодействия геополитических и национальных субъектов от социокультурных факторов. Но существует аспект коллективной безопасности, который имеет глобальный и универсальный характер, который действует не только между независимыми политическими субъектами, но и внутри социокультурной системы, и который еще никак не обсуждается не только в политических кругах, но не является предметом внимания научного сообщества. Вместе с тем, он имеет решающую роль в обеспечении жизнеспособности любой социальной системы. Как представлялось на протяжении человеческой истории, основным фактором достижения стабильности и защищенности человеческой популяции от различного рода опасностей является научно-техническая оснащенность. Однако, как показывают исторические исследования, в истории человечества погибло множество общественных систем, не оставивших после себя ничего, кроме археологического материала, имеющих довольно совершенную (соответственно своему времени) технологическую культуру. Само по себе наличие техники порождает большое количество как гуманитарных, так и организационных проблем. Первым обнаружил эту закономерность российский философ А.П.Назаретян, который писал, что «Растущий технологический потенциал делает социальную систему менее зависимой от состояний и колебаний внешней среды, но вместе с тем, более чувствительной к состояниям массового и индивидуального сознания». Назаретян сформулировал эту зависимость в виде закона: «закон техно-гуманитарного баланса – состоит в том, что чем выше мощь производственных и боевых технологий, тем более совершенные средства сдерживания агрессии необходимы для сохранения социальной системы».

Назаретян в своем исследовании сосредоточился на анализе человеческой агрессии и средствах ее сдерживания. Выведенный им закон имеет отношение не только к международным действующим субъектам и межнациональным и геополитическим взаимодействиям. Этот закон действует и внутри социокультурной системы, так как агрессия может быть направлена как вне, так и внутрь социума. И если предшествующие исторические социальные системы имели возможность перенаправлять человеческую агрессию на внешнего врага – другие этнические, национальные, идеологические системы, то в эпоху глобальных процессов мир перемешался – общество стало мультикультурным, полиэтничным, деидеологизированным. Объект человеческой агрессии оказался внутри социальной системы, следствием чего стал стремительный рост терроризма, адекватных средств сдерживания которого пока не создано. Террорист, оснащенный современными боевыми технологиями, представляет большую опасность, чем легализованные воинские структуры и не может быть локализован и нейтрализован никакими средствами оборонного назначения. Современными политиками признано, что военный потенциал представляет собой, главным образом, средство сдерживания, а вовсе не обеспечения реальной безопасности. В настоящее время технологическая оснащенность и свойства боевых технологий человечества таковы, что выживаемость не только локальной социальной системы, но и всего человечества стали зависеть не от количественного фактора (величина армии), не от материально-технического уровня (оснащение армии), и не только от информационного обеспечения, а от действий локальных групп и даже одиночек, заполучивших какими-либо средства наиболее разрушительный ресурс. Поэтому в

современном мире необходимым элементом системы коллективной безопасности является программа обеспечения организационной и психологической безопасности.

Понятие коллективной безопасности шире, чем защита от агрессии, как внутренней, так и внешней. Создание МЧС является следствием осознания факта, что опасность для социума может исходить как от социальной, так и естественной среды. Но если, для обеспечения безопасности от природных катаклизмов достаточно научно-технического потенциала, то на современном уровне технической оснащенности человечества все большую роль играет антропогенный фактор, который не может быть урегулирован исключительно научно-техническими и организационными средствами. Все большая техническая оснащенность человечества создает все большие экологические проблемы. Вместе с тем, отказаться от использования естественных ресурсов не представляется возможным. Поэтому закон сформулированный А.П.Назаретяном, как оказалось, выходит за пределы инструмента сдерживания агрессии. В истории человечества существовало много обществ, не справившихся с собственной технологической мощи и погибших от экологической катастрофы. Поэтому в настоящее время закон техно-гуманитарного баланса необходимо расширить и формулировать следующим образом: Чем совершеннее и эффективнее средства взаимодействия человека с природой, тем совершеннее и эффективнее должны быть средства регулирования этих отношений: информационные (знания), организационные (институты) и этические (нормы).

Попов П.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

ПОЛИТИЧЕСКИЕ ФАКТОРЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

Информационно-психологическая безопасность государства и социума – такое состояние системы управления, в котором у государственно-социальных институтов существует возможность и способность к самосохранению, имеются гарантии, обеспечивающие их устойчивое развитие и защиту от внутренних и внешних угроз, оказывающих на данные образования деструктивное информационно-психологическое воздействие (ИПВ).

В этом случае ИПВ по степени влияния может распределяться, например, на:

– информационно-психологические угрозы;
– информационно-психологическую агрессию;
– информационно-психологическую войну.

В качестве целей ИПВ можно выделить:

– разрушение ценностей противостоящей стороны, в первую очередь антагонистических, для их замены на собственные;
– разрушение защитного потенциала противника;
– подчинение ресурсов противника для их использования в собственных интересах;

При этом ИПВ обладает рядом существенных преимуществ по сравнению с другими видами воздействия (психотронным, психофармакологическим, психофизическим и др.), используемыми для оказания влияния на выбранный объект:

– непрерывность процесса, с самого начала до достижения требуемого результата и далее, в том числе, как в мирное время, так и в период вооруженного противодействия;
– непрогнозируемые масштабы последствий, начиная с получения влияния на конкретного индивида до подчинения отдельных государств и систем их управления, от экстремистской группировки до надгосударственного образования террористического толка;
– отсутствие общепринятых международных или национальных юридических или моральных норм и ограничений на средства и способы ИПВ и, в этой связи, отсутствие адекватных механизмов правовой защиты;
– практическое отсутствие действенных государственных и общественных механизмов прогнозирования, выявления и нейтрализации негативных ИПВ и устранения их последствий, и как следствие, отсутствие возможности противодействия использованию ИПВ до того момента, как оно будет применено в отношении объекта;
– максимальная степень скрытности «заказчика» и «организатора» ИПВ;
– может осуществляться в условиях как «информационного шума», так и «информационного вакуума».

Политическими факторами, усиливающими угрозы негативного ИПВ могут являться:

– изменение политической обстановки, как в отдельно взятой стране, так и в целом регионе;
– информационная экспансия со стороны ряда развитых стран (США, Великобритания, Германия, Израиль), осуществляющих глобальное информационно-пропагандистское воздействие в целях распространения мировоззрения, политических и духовных ценностей и идеалов «либерально-демократического» мира;
– провоцирование крупномасштабных конфликтов между государствами, этносами, конфессиями и другими видами сообществ;

– разрушение ранее существовавшей командно-административной системы государственного управления, политико-идеологической сферы, а также сложившейся системы обеспечения безопасности страны;

– низкий уровень, политической, правовой и информационной культуры в государстве и обществе.

Источниками угроз информационно-психологической безопасности для государства, общества, различных социальных систем, являются субъекты информационного противоборства:

– государства, их коалиции и союзы;

– международные и неправительственные организации;

– негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;

– транснациональные корпорации;

– виртуальные социальные сообщества;

– медиа-корпорации (СМИ и МК).

Пронин А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПРОПАГАНДИСТСКАЯ ДЕЯТЕЛЬНОСТЬ ЭКСТРЕМИСТСКИХ ОРГАНИЗАЦИЙ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

В условиях обострения международной геополитической ситуации особое значение обретает необходимость анализа информационно-пропагандистской деятельности, проводимой различными экстремистскими организациями.

Особую актуальность данный вопрос имеет в связи с интенсивной деятельностью представителей исламистских и националистических группировок, активно использующих масс-медиа в целях разжигания межнациональной и межрелигиозной розни, организации протестных и повстанческих движений. При этом свою силу подобные организации демонстрируют путем проведения акций устрашения и тиражирования совершаемых ими актов насилия.

На наш взгляд, благодаря развитию современных электронных СМИ, экстремистские группировки получили расширенные возможности оказания информационного и психологического воздействия на различные категории населения России и других стран. Доступность глобальной сети «Интернет», развитие социальных сетей и появление современных портативных устройств, позволяющих хранить, передавать и воспроизводить различные виды информации, предоставили деструктивным элементам небывалый потенциал по распространению текстовых, графических, видео- и аудиоматериалов идеологического содержания.

Подобная пропагандистская деятельность экстремистских организаций способствует радикализации взглядов отдельных групп индивидуумов, которые в дальнейшем могут совершать попытки дестабилизации обстановки в различных регионах России и за ее пределами.

Кроме того, совершенствование методов и средств информационно-пропагандистской работы значительно повысило эффективность вербовки новых членов радикальных националистических и религиозных организаций. В частности, в их ряды вступают абсолютно, на первый взгляд, не склонные к подобным действиям лица различной национальной и государственной принадлежности.

Необходимо отметить, что риску подвергнуться информационному воздействию экстремистов подвержены жители всех регионов РФ, что обусловлено широкой растиражированностью распространяемых радикальными организациями материалов в современном информационном пространстве. Зачастую невольно их распространению содействуют официальные СМИ.

Наиболее ярким современным примером использования масс-медиа в террористических целях является деятельность организации «Исламское государство Ирака и Леванта», в значительной мере ответственной за эскалацию военно-политического кризиса на Ближнем Востоке.

Применительно к нашему региону следует отметить, что крайне негативное воздействие на психоэмоциональное состояние населения РФ оказывала деятельность националистических организаций, активно участвовавших в событиях 2013-2015 гг. в Украине.

Требуется подчеркнуть, что на данный момент наиболее чувствительной к негативному информационному воздействию целевой аудиторией в России является население Крымского федерального округа. Неоднозначное отношение крымско-татарского и украинского населения полуострова к воссоединению с Россией и многолетняя работа радикальных организаций среди местных жителей делают регион своеобразной «зоной риска», к которой привлечено пристальное внимание мировой общественности.

Помимо этого, геостратегические средства политического и экономического давления на РФ отрицательно влияют на состояние информационно-психологической безопасности населения страны в целом. Экономические санкции, нестабильность рынков углеводородов и валюты создают

предпосылки для формирования у россиян атмосферы неуверенности в будущем, что препятствует стабильному развитию государства и общества.

Таким образом, государственная политика в области обеспечения информационно-психологической безопасности населения регионов России должна быть гибкой и комплексной и формироваться с учетом современных условий развития глобального информационного пространства. Одной из основных задач при этом является противодействие деятельности радикальных религиозных и националистических организаций, отрицательно влияющей на психическое и эмоциональное состояние населения России. Кроме того, мониторинг данной деятельности, ее ограничение позволят ослабить существующие тенденции к радикализации отдельных категорий российских граждан.

Свешникова Н.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет

ПСИХОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Проблема влияния информации на состояния больших групп людей и их настроения в современном обществе является одной из актуальных в современных исследованиях. Это связано с гетерохронным развитием социокультурных систем современности, возрастанием ситуации неопределенности будущего, изменением роли информационных технологий в системе коммуникации и жизнеобеспечения общества. Кастельс, обсуждая особенность новой социальной организации, особо отмечает, что генерирование, обработка и трансляция информации стали фундаментальными источниками производительности и власти. Многие исследователи рассматривают современную ситуацию как эпоху «информационного фундаментализма» или «информационного тоталитаризма». Информационные войны – качественно иной уровень политического, социокультурного и экономического противостояния в мире. Информационная война ведется в пространстве «естественное – виртуальное», создавая качественное отличие от классических идеологических войн. Проблема информационной безопасности становится одной из основополагающих для целей развития, как общества, так и отдельной личности.

Внимание исследователей к феномену информационной безопасности также объясняется необходимостью внедрения новых технологий информационного взаимодействия/противостояния, разработки новых стратегий социального и политического поведения с учетом психологических аспектов поведения и мотивации. Сегодня востребованы приемы, позволяющие более эффективно вести внешнюю и внутреннюю политику государства, новейшие технологии и разработки в области управленческой деятельности. Существует потребность в новых методах, имеющих более широкие возможности и эффективность психологического воздействия.

Потенциал информационного воздействия весьма широк: от формирования общественного мнения до реализации социального контроля и управления. Информационную безопасность необходимо рассматривать системно, учитывая различные уровни обеспечения (личностный – социальный), способы реализации, механизмы и эффекты воздействия. Ведущая роль сегодня отводится новым технологическим условиям - интернет-коммуникации, электронные СМИ, для которых не существует границ. Важно, с нашей точки зрения, отметить, что новые технологические возможности предопределили и отличие характера, условий влияния, и субъекта воздействия. Современные данные психологических исследований позволяют полагать, что стратегия информационного воздействия в большей степени базируется на «субъект-субъектной» парадигме, принципах информационного разнообразия и многообразия.

В современном обществе СМИ выступают в качестве проводников массовой культуры и определяющим образом влияют на формирование ценностных установок, стиля и образа жизни населения. Это очень важный фактор формирования социокультурной идентичности как индивидуальной, так и коллективной (групповой) в ситуации все возрастающего взаимопроникновения культур. Проблема понимания своей и чужой культуры, транслируемой посредством печатной продукции, фильмов, рекламы, интернета и пр., как исследовательская задача представляет собой новый качественный уровень изучения воздействия информации. Такой подход открывает перспективы в представлении о возможностях трансформации смыслового пространства, пределов таких изменений. Особое внимание уделяется форме межиндивидуального существования смыслов в пространстве коллективной ментальности. При этом весьма важным аспектом является то, что коллективные смыслы, присущие социальной общности, определяют становление смысловых полей членов этой общности, но и сами коллективные смыслы могут трансформироваться при взаимодействии как внутри общности, так и за ее пределами. Смысловое поле социальной общности представлено в виде образно-символического воплощения. Большую роль в принятии и понимании, трансформации смысловых полей играет ситуация коммуникации, возраст, общий уровень компетентности, социальный опыт, профессиональные особенности, воспитание и др.

Худяков А.И., Худякова Е.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена

ПСИХИКА. ИНФОРМАЦИЯ. БЕЗОПАСНОСТЬ

Безопасность — фундаментальная человеческая потребность, и это убедительно аргументировано во многих психологических теориях. Например, согласно иерархии мотивационных образований личности А.Маслоу, высшие человеческие потребности — в самоактуализации, в признании и оценке, в любви и привязанности — реализуются на основе удовлетворения физиологических (витальных) потребностей человека, а также присущей каждому из нас потребности в безопасности. Вместе с тем посвященных проблемам психологической безопасности исследований сравнительно мало, так что соответствующая проблематика не принадлежит к настоящему времени к числу базовых для психологической науки.

Информационно-психологическая безопасность Этот аспект информационной безопасности связан в первую очередь с воздействием недоброкачественной информации на психологическое состояние личности, что несёт угрозу интеллектуальному, духовно-нравственному состоянию человека, а также угрозу его физическому здоровью. Информационно-психологическую безопасность в общем виде можно определить как состояние защищенности психики от разрушительного воздействия на сознание информационных факторов. Применительно к конкретному человеку информационно-психологическая безопасность – это состояние защищенности психики человека, обеспечивающее его целостность как социального субъекта, возможность адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий. Задача обеспечения ИПБ должна решаться на уровне государства, общества и на уровне самой личности. Источников угроз информационно-психологической безопасности существует великое множество, и проявляться они могут через СМИ, разные направления массовой культуры, воспитание, личное общение, образовательные системы и культовые образования. Выделяют несколько видов так называемой «вредоносной» информации, могущей нанести серьёзный вред психике человека. К ней можно отнести:

– информацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду;
– призывы к войне;
– пропаганду ненависти, вражды и превосходства;
– посягательство на честь, доброе имя и деловую репутацию людей;
– рекламу (недобросовестную, недостоверную, неэтичную, заведомо ложную);
– информацию, оказывающую неосознаваемое деструктивное воздействие на психику людей.

Какие же неблагоприятные информационные факторы привели к тому, что возникли угрозы для личности? Основной из них является так называемый «информационный взрыв» или лавинообразное увеличение всех видов традиционной, печатной информации (научной, научно-технической, экономической, научно-популярной, юридической, коммерческой, эстетической и так далее). Еще большими темпами развиваются электронные информационные ресурсы, масштабы которых трудно поддаются измерению. Количественный рост информации привел к тому, что личность не может воспринять, осмыслить, систематизировать даже те источники информации, которые необходимы ей в профессиональной деятельности. Этот фактор породил избыток, перенасыщение информационной среды. Большое количество информации, даже без учета ее качественных характеристик, отрицательно влияет на личность.

Как же бороться с этими явлениями реальной жизни и надо ли это делать? Психика человека может выдерживать определенное время достаточно большие нагрузки на нее без видимых повреждений, компенсировать нежелательные воздействия. Но в определенный момент эти нагрузки могут превысить верхний абсолютный порог, и тогда возможно возникновение необратимых последствий. Этим проблемам и посвящен настоящий доклад.

Шацкая В.И.
Россия, Санкт-Петербург, Северо-Западное отделение Академии геополитических проблем

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА НАСЕЛЕНИЕ (НА ПРИМЕРЕ УКРАИНСКОГО КРИЗИСА И РАЗВЕРТЫВАНИЯ ГЛОБАЛЬНОЙ СИСТЕМЫ ПРО США)

В настоящее время в обязательном порядке проводится информационно-психологическая поддержка военных операций и внешнеполитических действий США. При этом США стремятся достичь информационного превосходства в мировом пространстве. Для этих целей используется как дезинформация и вброс специально обработанной информации в СМИ, так и создание благоприятного общественного мнения как внутри самих США, так и в странах союзниках. На примере украинского кризиса и развертывания глобальной системы противоракетной обороны США очевидна мощная пропагандистская кампания Вашингтона и союзников, направленная на убеждение в правильности и необходимости принимаемых США и НАТО решений. Такими «правильными»

решениями выступают, например, увеличение численности Сил реагирования НАТО до 40 тыс. человек, открытие шести передовых координационных центров НАТО в Эстонии, Литве, Латвии, Румынии, Польше, Болгарии, планы США разместить новые ядерные авиабомбы B61-12 в Германии, размещение тяжелой военной техники в странах Балтии, Восточной Европе и Германии и т.д.

В связи с откровенной несостоятельностью утверждений США о ракетной угрозе со стороны Ирана и КНДР, что лишний раз подтвердило и новое соглашение по иранской ядерной программе, Вашингтон подвергает и некоторой корректировке информацию, которая посредством СМИ и интернета транслируется в массы. При этом схожие приемы используются при освещении гражданской войны на Украине. Для этих целей США:

1. Последовательно создают образ «агрессора» в лице России. Практически во всех наиболее известных западных газетах и журналах, в материалах, посвященных России, обязательно фигурируют слова и словосочетания негативного характера: «российская угроза» и т.д. Кроме того, активно нагнетается ощущение страха у стран-членов НАТО.

2. Представление России в СМИ как непредсказуемого соседа для стран Европы, и необходимостью в связи с этим укреплять безопасность Европы при помощи американских баз и технологий.

3. США под разными предлогами провоцируют волны антироссийских настроений, настойчиво обращаясь к исторической памяти. Особенно это характерно для взаимоотношений со странами Балтии и Украиной.

4. Вероятно применение материального поощрения при присоединении союзников к планам США. В данном случае, в обмен на развертывание американских элементов ПРО США на своих территориях, страны-участницы могут ожидать подписания выгодных контрактов, либо выделение средств на оборону данных государств.

Эти и другие способы соответствуют лишь одной цели: выйти сухими из воды на мировой арене и правильно подготовить зарубежное и собственное население к возможным в будущем боевым действиям на территории Европы, если в таковых возникнет необходимость.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

Абиссова М.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ И СЕРВИСЫ ОБУЧЕНИЯ ДИСЦИПЛИНЕ «МИРОВЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ» В ВЫСШЕЙ ШКОЛЕ

При обучении студентов дисциплине «Мировые информационные ресурсы» ни в ее содержании, ни в конкретных приемах методики ее преподавания нельзя обойти стороной вопросы такой актуальной ныне области знаний как информационная безопасность (ИБ).

В особенности, учитывая необходимость практической демонстрации различных современных сервисов Интернет, включая облачные технологии. Также в содержании этой дисциплины нельзя не сказать о современном социокомпьютинге, как понятии, описывающем многообразное использование, распространение, роль и влияние информационно-компьютерных технологий в современном социуме. Нельзя не затронуть социокомпьютинг вообще и ИБ в социокомпьютинге в частности.

К сожалению, степень информатизации и компьютеризации в большинстве современных вузов России не превосходит соответствующего уровня среднестатистического представителя современного социума в повседневной жизни. Что делает особенно актуальным изучение ИБ именно на уровне социокомпьютинга. Теперь о том, что такое сервисы обучения (СО) вообще и СО дисциплине «Мировые информационные ресурсы» в частности.

В последнее десятилетие в ряде научных публикаций, посвященных таким областям знаний, как информатика и информационные технологии (ИТ) говорится о фактическом возникновении новой науки – науки о сервисах, управлении и инжиниринге, или по английски - Service Science, Management and Engineering (SSME). Сам термин SSME предложен исследовательским центром IBM как обозначение для новой версии науки Computer Science, которая в России известна как информатика. Причем особо отмечается отсутствие общего определения понятия сервиса, необходимого для фундаментальных научных исследований в этом направлении. П

риблизительно в этот же период нами (автором данных тезисов и его коллегами) развивалась инновационная сервисная методология по отношению к процессу обучения студентов информатике и ИТ. В качестве основы этой методологии был предложен новый педагогический термин – СО. Предположим, что в процессе обучения возникает некоторая задача Р, являющаяся следствием именно обучения. Здесь мы намеренно не конкретизируем о каком именно обучении идет речь (обучение чему?, обучение кого?), мы имеем в виду собирательное понятие обучения.

Под сервисом обучения S мы будем понимать набор из такой задачи Р и непустого множества М ее решений. Введенное нами понятие СО является дополнением к известным в педагогике методическим системам обучения и близко по значению понятию сервиса из области ИТ. СО с учетом ИБ разрабатывались автором и коллегами, а затем практически внедрялись в различные курсы обучения информатике и ИТ различных вузов.

На наш взгляд, особо значимы среди них СО по курсу «Мировые информационные ресурсы». Нами применялись многообразные СО. Среди них как концептуальные СО комментирования, отбора учебного материала, так и информационно-технические СО с использованием различных электронных носителей, программ, файлов данных различных форматов, облачных сервисов. Какую же реальную пользу понятие СО может принести?

Часто перед вузом, кафедрой или отдельным педагогом ставится некоторая нетривиальная задача, причем ее решение ему не известно, но его необходимо оперативно найти и реализовать. Таковыми, например, являются задачи интеграции педагогических и информационных технологий (ПТ и ИТ). Тогда фактически отдельным педагогом или некоторой рабочей группой специалистов и строится СО. СО направлены главным образом на оперативное решение возникающих в процессе обучения нетривиальных задач. Фиксация в рамках СО и задачи, и найденных ее решений позволяет использовать СО неоднократно в аналогичных ситуациях. Фактически СО строятся педагогами весьма часто.

Таким образом, СО - это независимая от нас объективная педагогическая реальность. В качестве примера СО приведем сервис параллельной компьютерной сети. Проблема: При изучении разделов, связанных с ИБ необходимо проводить на компьютере такие эксперименты (например, по

установке и настройке антивирусных программ и файрволов), при которых может пострадать безопасность не только данного компьютера, но и других в компьютерной сети вуза.

Решение:

Способ 1. Ограничиться лекциями и рефератами.

Способ 2. Потребовать от администрации организации специального компьютерного класса для проведения таких занятий. Этот класс не должен быть подсоединён к компьютерной сети вуза, и выход в Интернет должен быть свой.

Способ 3. Отсоединить два компьютера от сети вуза или воспользоваться двумя ноутбуками преподавателя или студентов. Между ними организовать сеть. Выход в Интернет организовать через сотовую связь. К обоим компьютерам подсоединить проекторы, чтобы студенты на больших экранах видели всё происходящее. На эти компьютеры последовательно сажать разных студентов.

Как показывает наш опыт, такие СО способствуют существенному улучшению качества подготовки в высшей школе в направлении ИТ вообще и ИБ в частности.

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

КОМПЛЕКС ПРОГРАММ ДЛЯ АНАЛИЗА ДОСТИЖИМОСТИ КРИТИЧНЫХ ДОКУМЕНТОВ И ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

В рамках комплекса «информационная система — персонал — критичные документы» были предложены две модели имитации социоинженерных атак злоумышленника на пользователей информационной системы: на социальном графе пользователей и в комплексе «ИСПКД». Данные модели дают оценку защищённости пользователей от социоинженерной атаки злоумышленника на основе связей между пользователями.

Был создан прототип комплекса программ, реализующий алгоритмы, позволяющие проводить автоматизированный анализ достижимости критичных документов и защищенности пользователей информационных систем от социоинженерных атакующих воздействий злоумышленника. Прототип комплекса программ был разработан на языке C# с применением MySQL Server. В состав прототипа комплекса программ входят следующие программные модули:

1. модуль работы с базой данных;
2. модуль создания и наполнения информационной систем;
3. модуль визуализации информационной системы;
4. модуль преобразования психологических особенностей личности в профиль уязвимостей пользователя;
5. модуль имитации распространения социоинженерной атаки злоумышленника в социальном графе пользователей информационной системы;
6. модуль имитации социоинженерной атаки злоумышленника на пользователей информационной системы, с учетом профиля уязвимостей пользователя;
7. модуль выделения групп пользователей информационной системы для последующей работы с ограниченной группой пользователей.

Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

КОМПЛЕКС «КРИТИЧЕСКИЕ ДОКУМЕНТЫ — ИНФОРМАЦИОННАЯ СИСТЕМА — ПЕРСОНАЛ —ЗЛОУМЫШЛЕННИК»

В диссертационной работе А.А. Азарова был рассмотрен комплекс «информационная система — персонал — критичные документы», где были предложены две модели имитации социоинженерных атак злоумышленника на пользователей информационной системы: на социальном графе пользователей и в комплексе «ИСПКД». Данные модели дают оценку защищённости пользователей от социоинженерной атаки злоумышленника на основе связей между пользователями, в тоже время в данных моделях не учитывается профиль компетенции злоумышленника. Предлагается рассмотреть комплекс «критические документы — информационная система — персонал — злоумышленник» (комплекс «КДИСПЗ») вместо комплекса «ИСПКД», который позволит увеличить точность оценки защищенности пользователей информационных систем от социоинженерных атак за счет вероятностных оценок действий злоумышленника.

Профиль компетенций злоумышленника (ПКЗ) имеет большое значение наравне с профилем уязвимости пользователя (ПУП) для оценки успешности атакующего воздействия. Важность изучения особенностей двух сторон взаимодействия – того, кто влияет, и того, на кого влияют, – подчеркивается в научной литературе. Известный специалист в области психологии влияния Роберт Чалдини в своей монографии отмечал, что изучать психологию уступчивости он начал с серии экспериментов, позволяющих выяснить, какие принципы и особенности лежат в основе податливости

в отношении просьб или требований, но вскоре понял, что нужно изучать и вторую сторону данного процесса. Он назвал этих людей «профессионалами уступчивости», поскольку, они хорошо знают, как построить взаимодействие, чтобы собеседник уступил и выполнил просьбу или требование. «Они знают, что срабатывает, а что — нет <…>. Такие люди стараются, во что бы то ни стало, заставить окружающих уступить, от этого зависит их успех в жизни. Те, кто не знает, как вынудить людей сказать «да», обычно терпят поражение; те же, кто знает, — процветают.» Р. Чалдини в результате своих наблюдений выводит шесть основных принципов влияния: принцип последовательности, принцип взаимного обмена, принцип социального доказательства, принцип авторитета, принцип благорасположения, принцип дефицита. Однако, в число главных принципов не было включено правило «личного материального интереса», которое автор рассматривает как «некоторую аксиому, которая заслуживает признания, но не подробного описания».

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

АЛГОРИТМЫ РАСЧЕТА ВЕРОЯТНОСТНЫХ ОЦЕНОК ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА НА ОСНОВЕ МАРКОВСКИХ СЕТЕЙ

Доклад посвящен рассмотрению алгоритма расчета вероятностных оценок защищенности пользователей информационных систем от социоинжереных атакующих воздействий злоумышленника. Предлагается к рассмотрению алгоритм на основе Марковских сетей. Данный алгоритм предполагает построение матрицы, содержащей вероятностные оценки успешности социоинженерных атакующих воздействия злоумышленника на пользователей информационной системы. Также данная матрица содержит вероятностные оценки доступа пользователей к критичным документам, хранящимся в информационной системе. Вероятностные оценки успешности социоинженерных атакующих воздействий злоумышленника строятся на основании профиля уязвимостей пользователя, связанного с психологическими особенностями личности, а также на основании профиля компетенций злоумышленника. Ресурсы злоумышленника и его предполагаемые компетенции содержатся в профиле компетенций злоумышленника. Итоговая вероятность успеха совершенной социоинженерной атаки злоумышленника предлагается рассчитывать возводя рассматриваемую матрицу в степень, соответствующую времени, затраченного злоумышленником на совершение атаки. Предполагается, что одно социоинженерное атакующее воздействие злоумышленника требует одну единицу времени.

Баев В.А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ХРОНОТИПА ПОЛЬЗОВАТЕЛЯ ПО ЕГО ЦИФРОВЫМ СЛЕДАМ

Задача выявления характеристик профиля пользователя социальных медиа по оставленных им цифровых следам является одной из наиболее актуальных в социальном компьютинге, одним из наиболее распространенных ее применений является идентификация взлома пользователя. В рамках данной работы предложен подход к определению хронотипа пользователя по его цифровым следам в Twitter. В работе выделены признаки на основе использования определенной лексики: потребление кофе, склонность к депрессии, частота положительно и отрицательно окрашенных сообщений. Результаты работы превосходят существующие аналогичные результаты по определению хронотипа пользователя на основе времени публикации твитов.

Блюм В.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

МАСТЕР-ИНДЕКС ПАЦИЕНТОВ ДЛЯ МОДЕЛИ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ И ЕГО ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ

Предложена дискретно-событийная модель потока первичной медицинской информации в системе здравоохранения. Модель рассматривается как математический образ вновь создаваемого федерального сервиса «Интегрированная электронная медицинская карта» и предназначена для анализа процессов формирования и использования полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации.

Рассмотрен алгоритм и технология формирования индекса пациента (идентификатора ИЭМК), а также методы приведения существующих идентификационных признаков к индексу пациента, исключающие ошибки идентификации ИЭМК.

Блюм В.С., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ВЕКТОРНО-СОБЫТИЙНАЯ МОДЕЛЬ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ И ЕЁ СОЦИАЛЬНОЕ ЗНАЧЕНИЕ

Система здравоохранения, как социальный институт, переживает этап информационного взрыва. Центральной задачей системы охраны здоровья является профилактика и борьба с вторжениями болезней в жизнь общества. Решение этой задачи предполагает обладание полной, достоверной и доступной для автоматизированной обработки информации о состоянии здоровья каждого гражданина и общества в целом. Источники первичной медицинской информации (врачи и диагностические лаборатории) ежегодно генерируют более четырёх терабайт данных. Эта цифра непрерывно растёт. Требования к достоверности и полноте медицинской информации приводит к необходимости её дублирования и интеграции. Одним из основных процессов интегрирования медицинских данных в современной системе здравоохранения стал национальный проект «Интегрированная электронная медицинская карта» (ИЭМК). При успешной реализации этого проекта его влияние на жизнь общества трудно переоценить. В этой связи, разработка и исследование моделей сложного, динамичного объекта, каким является ИЭМК, становится насущной задачей. Предложена векторная информационно-событийная модель ИЭМК, способная обеспечить оперативный мониторинг общественного здоровья и информационную безопасность персональных медицинских данных, как на региональном, так и федеральном уровне.

Валькова Т.В., Суровенко И.А., Влащенко А.О,
Россия, Санкт-Петербург, 9 отдел БСТМ ГУ МВД России по СПб и ЛО,

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГРАЖДАНИНА.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ «САМОГО СЕБЯ»

Представьте себе, что почти треть жителей планеты ежедневно заходит в сеть Интернет, т.е. ежедневная «онлайн» аудитория составляет не меньше 2,8 млрд человек, что составляет около 40% всего населения Земли (на 2015 год). Учитывая темпы, динамику и географию распространения, Интернет скоро станет доступен и в самых отдаленных уголках нашей планеты. Так приведу немного свежей статистики.Рост интернет-аудитории в 2014 году составил 8%, по сравнению с 2013 годом. Основным источником новой Интернет аудитории остаются развивающиеся страны. К примеру, в 2014 году в Индии число пользователей Сети увеличилось сразу на 33%, по сравнению с 2013 годом. В Китае аналогичный показатель составил 7%, в США — 2%, в Бразилии — около 4%. Вполне логично, что больше всего пользователей Сети — в Азии. Стоит отметить, что все большее количество людей выходит в Сеть через смартфоны. А пользователей мобильных телефонов сейчас уже 5,2 миллиарда человек, это 73% населения Земли. 40% этой аудитории используют смартфоны. Благодаря большому числу пользователей «умных телефонов» растет и трафик с мобильных устройств. Так, в 2014 году рост составил сразу 69%. Россия входит в топ-15 стран по числу абонентов мобильной связи. В РФ около 23% пользуются смартфонами. Никто не ставит под сомнение практическую пользу современных технологий, различных гаджетов, устройств, которые зачастую не имеют смысла и не могут быть реализованы без существования Интернета, однако необходимо выйти из «кокона безопасности», и понять, что информационная бомба может быть заложена здесь и сейчас, прямо в Вашем кармане (в котором вероятно лежит Ваш смартфон), и когда она сработает против Вас, что то предпринимать будет уже поздно.

Миллионы людей оставляют в сети Интернет, в т.ч. социальных сетях свои реальные данные, имена, фамилии, дату рождения (женщины могут скинуть пару лет), адреса, номера телефонов, сведения о друзьях, близких родственниках и другую значимую информацию об их личной жизни, и делают это добровольно и открыто. Музыка, – которая, кстати, многое о Вас говорит. Книги, которые Вы читаете – тоже многое о Вас говорит. Список Ваших друзей – говорит о Вас почти всё!Важный вопрос, это «кто ваши друзья?». Потому, что если я знаю, кто ваши друзья, я знаю о вас все что нужно. А в этом сама суть социальных сетей, таких как «ВКонтакте», «Facebook», «Одноклассники». Где Вы живете, Ваши хобби, Ваши дети, Ваши родители, Ваши братья и сестры, родственные связи, и…фотографии, фотографии, фотографии. Кому эта информация интересна и нужна больше всего? Все просто! Это маркетологи, сотрудники спецслужб в т.ч. полиции, частные детективы и мошенники!

Так, например распространенное мошенничество, в котором злоумышленник по телефону парадирует голос близкого родственника (сына, дочери) потерпевшего, выпрашивая (понимать «вымогая») денежные средства для «откупа» того же родственника, попавшего в ДТП, полицию (возможны др. причины), в большинстве случаев совершается с предварительной подготовкой и всевозможной разведкой о составе семьи, финансовом положении, психологии жертвы, которую злоумышленник может получить используя доступные Интернет ресурсы и социальные сети. И это лишь единственный пример из массива изощренных способов мошенничества в Сети с использованием Ваших данных.

Существуют множество Интернет ресурсов которые архивируют вводимые Вами в социальных сетях открытые данные, которые сохраняются даже после удаления источника, поэтому каждый раз, когда Вы собираетесь, опубликовать какую-либо личную информацию о Вас, задумайтесь над тем, не сможет ли она сработать против Вас.

Верещагин В.Л., Муллина Э.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТЯХ, ПОСТРОЕННЫХ НА КОММУТАТОРАХ CISCO

Опыт участия в аукционах последних трех лет показывает, что создание системы защиты для бюджетных организаций существенно варьируется по выделяемому финансированию: наибольшее количество денег получают администрации и существенно меньше выделяется для организаций. занимающихся социальным обеспечением. Чаще всего это обоснованно большей сложностью административных сетей, но при этом по-разному решается и проблема замены коммутационного оборудования, при условии, что оно не прошло сертификацию.

Последовательность проведения работ по созданию защищенной сети в большинстве случав подразумевает наличие ранее созданной и преобразование её в защищенную. Большой удачей, если посмотреть по России в целом, следует считать возможность включить администратору в свою бюджетную сеть коммутаторы Cisco– это и удобство, и надежность, и масштабируемость, и безопасность. Дальнейшее выполнение законодательства в области защиты персональных данных воспринимается Заказчиками как защита рабочих станций, установка межсетевых экранов, внедрение систем обнаружения вторжений и обеспечение антивирусной защитой, с учетом имеющей архитектуры сети. Заказ обследования и формирование проекта – это тот этап проектирования на котором возможны следующие подходы:

- сохранение архитектуры Cisco и защита серверов с рабочими станциями:
  1. с сертификацией коммутаторов;
  2. без сертификации коммутаторов;
- построение новой архитектуры без учета указанных коммутаторов.

Данная работа демонстрирует неправомерность сохранения несертифицированного оборудования даже при защите конфиденциальной информации, высокую стоимость сохранения оригинальной сети и неготовность Заказчика к исключению из имеющейся сети коммутационного оборудования, закупаемого, порой небольшими объемами в течении ряда лет.

В работе рассмотрено частичное решение задачи на маленьких сетях, когда стоимость создания первоначальной сети не выходит за границы суммы, возможной потратить единовременно без объявления конкурса, а также сложность её перестройки не подразумевает остановку работы на период более долгий, чем несколько дней.

Решения на крупных сетях, имеющих критичное значение (например, крупные медицинские центры федерального значения) в настоящий момент отсутствуют т.к. требуют вложений больше, чем возможно выделить службе управления заказами Заказчика даже за несколько лет.

Хорошим решением предлагается считать возможность быстрой сертификации прошивки коммутационного оборудования, размещенного на объекте. Технически это возможно выполнить при помощи инструментальных средств, позволяющих определять базовый код прошивок (т.н. «паспорт») и затем для новых модификаций прошивок в автоматическом режиме блокировать функции, отличающиеся от паспортных данных. Существуют программные комплексы, решающие частично эту задачу, например, довольно старый но качественный продукт «IRIDA», но решения, позволяющего снизить стоимость сертификации оборудования до доступного для каждой школы – в настоящее время нет и требуются новые идеи.

Опыт поиска решений на примере небольших сетей (до 100 рабочих мест и до десяти серверов) показывает, что уверенность Заказчика в возможности выполнить защиту без сертификации коммутаторов может быть поколеблена демонстрацией 2-х решений в конечном проекте, где одно подразумевает дорогостоящий расчет с сертификацией оборудования (для одной единицы стоимость может в несколько раз превышать стоимость проведения предпроектного обследования и разработки технического проекта) и второй – с заменой на коммутирующие сервера, работающие под сертифицированной операционной системой. Одной из целей основной статьи, к которой относятся настоящие тезисы, является демонстрация для заинтересованного круга читателей описанной проблемы и конкретных решений для наиболее распространенных по территории России типов сетей, включающих в свой состав оборудование на архитектуре intel, x86-64 и программном обеспечении фирмы Microsoft, сочетающееся с различными Linux-системами, применяемых для серверных решений и рабочих мест работников.

В работе приводятся примеры проектирования системы защиты 2-мя способами, каждый из которых содержит типовую схемы сети и её техническое описание.

Гейгер Г., Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ СИСТЕМ ЗАЩИТЫ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОБЪЕКТАХ

Существует задача формирования системы защиты на объекте в определенные сроки с заданным качеством защищаемой информации. Объект защиты представлен типовой иерархической компьютерной сетью, многопользовательская система, с рабочими местами и выделенным сервером. Предъявляемые требования к защите представляют собой размещение необходимых средств защиты информации, таких как СЗИ, САВЗ, МЭ, СОВ. Необходимо было решить задачу определения такой конфигурации из различных средства защиты, которая бы позволяла выполнить монтаж и установку в кротчайшие сроки, без конфликтов система защиты между собой, сохранением полной работоспособности сети и обеспечения заданного класса защиты конфиденциальной информации. В результате были проведены прикладные исследования с целью определения оптимального решения, обеспечивающего: надежность, скорость установки, оптимальность затрат.

Перечень средств задействованных в исследовании:

1. СЗИ АУРА 1.2.4;
2. СЗИ Secret Net 7;
3. СЗИ DallasLock 8.0;
4. САВЗ Dr.Web 10.0;
5. САВЗ Kaspersky antivirus;
6. САВЗ SSEP 7.7;
7. СОВ SSEP 7.7;
8. МЭ SSEP 7.7.

Был применен метод сравнения, подразумевающий последовательную установку и настройку на виртуальных и реальных стендах различных комбинаций СЗИ НСД + МЭ + СОВ + САВЗ. В результате было сформировано 9 вариантов комбинаций, в которых неповторяющимися были только межсетевые экраны и системы обнаружения атак по причине целевых установок использования на рабочих местах именно этих программных продуктов. Дальнейшие исследования подразумевают расширение линейки программных персональных экранов.

В статье приводится полный список конфигураций, в частности, были рассмотрены следующие:

1. «Станция №2» (СЗИ АУРА 1.2.4, САВЗ Kasperskyantivirus, СОВ SSEP 7.7;МЭ SSEP 7.7);
2. «Станция №6» (СЗИ SecretNet 7, САВЗ SSEP 7.7, СОВ SSEP 7.7, МЭ SSEP 7.7);
3. «Станция №7» (СЗИ DallasLock 8.0, САВЗ Dr.Web 10.0, СОВ SSEP 7.7, МЭ SSEP 7.7).

Результаты проведенных исследований: наиболее надежными при установке и по скорости настройки настройки в сочетании с другими средствами защиты стали СЗИ НСД «АУРА 1.2.4» (разработка «СПИИРАН») и «DallasLock 8.0» (разработчик ООО «Конфидент»):

1. «Станция №1» (СЗИ АУРА 1.2.4, САВЗ Dr.Web 10.0, СОВ SSEP 7.7;МЭ SSEP 7.7);
2. «Станция №9»(СЗИ DallasLock 8.0, САВЗ SSEP 7.7, СОВ SSEP 7.7, МЭ SSEP 7.7).

Наиболее экономически выгодной следует считать из рассмотренных конфигурацию «Станция №3» (СЗИ АУРА 1.2.4, САВЗ SSEP 7.7, СОВ SSEP 7.7; МЭ SSEP 7.7).

На основе полученных результатов были проведены успешные внедрения на объектах вариант конфигурации «Станция №1».

Не проводилась апробация на объектах конфигурации «Станция №9» по причине исключительной сложности приобретения программного изделия у разработчика для объектов, подходящих для защиты в рамках государственного заказа, при которой даже в случае выигрыша аукциона на поставку, компания-разработчик не способна поставить сколь угодно малое количество единиц товара по причине «перегруженности производства».

Левко Г.М, Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

АВТОРСКИЕ ПРАВА И ИХ ЗАЩИТА В СИСТЕМЕ ИНТЕРНЕТ

О нарушениях авторских прав в сфере Интернета известно всем без исключения: и пользователям Интернета, и самим авторам.

Защищаясь от нарушений, автор может разместить свой материал на коммерческой веб-странице, доступ к которой возможен при условии внесения на соответствующий счет определенной денежной суммы. Зачисление денег на счет совпадает с зачислением плательщика в список лиц, которым открыт доступ к данной странице. Поэтому существует возможность «отследить» дальнейшее размещения материала, взятого с коммерческого сайта, где-либо еще в Интернете.

Можно защищать авторские права в Интернет посредством записи информации с Web-страниц на лазерный диск при последующем его депонировании в хранилище, которое называют Web-депозитарий.

Для этого лицо подает заявление об авторстве с указанием произведения, его описания, фиксируется дата приема, оформляется свидетельство о принятии объекта. Однако дата депонирования будет доказательством, лишь того факта, что в указанное время заявитель обладал копией объекта.

В некоторых сегментах Сети эффективно используется способ защиты в виде «водяных знаков» в электронных копиях фотографий и изображений. С помощью специального программного обеспечения встраивается скрытый код определенного формата в файлы. При визуальном рассмотрении не видно закодированных обозначений (ими могут быть имя автора, год издания, знака авторства). Водяные знаки устойчивы к любым операциям над изображением и при применении специального программного средства можно доказать, что файлы содержат дополнительную информацию, указывающую на лицо, ее записавшее.

Следует отметить, что нарушаются и права авторов сайтов – описаны случаи, когда материалы, появившиеся сначала в Интернете, были скопированы и воспроизведены в печатном издании.

Самборский И.М., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ВЫЯВЛЕНИЕ АККАУНТОВ, НЕ ПРЕДСТАВЛЯЮЩИХ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Одной из современных угроз для цифровой безопасности является рост профилей в социальных медиа, которые не ведутся от лица их хозяина. Выявлению одного из типов таких профилей — ботов, посвящен целый пласт исследований. Настоящая работа посвящена определению двух других видов подобных профилей: аккаунтов, ведущихся от лица организаций, а также аккаунтов выдуманных персонажей.

Для классификации использована выборка профилей из русско- и англо-язычного сегментов Твиттера. Классификаторы обучались как на основе частоты употребления слов, так и на основе более сложных численных характеристик речи. Классификатор, основанный на последних, превзошел базовые модели, а также уже существующий алгоритм.

Святкина М.Н.
Россия, Москва, Московский государственный технический университет им. Н.Э.Баумана

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ КОГНИТИВНОЙ ГРАФИКИ В СИСТЕМАХ МОНИТОРИНГА СЛОЖНЫХ ТЕХНИЧЕСКИХ ОБЪЕКТОВ

В промышленности, на производстве и транспорте одной из ключевых проблем остается задача обеспечения безопасности. Многие процессы в этих сферах являются потенциально опасными и при возникновении аварий приводят к человеческим жертвам, к значительному материальному и экологическому ущербу. Согласно результатам анализа большинства аварий и происшествий на всех видах транспорта, в промышленности и энергетике в XX веке были получены следующие данные: в 60-х годах ошибка человека была первоначальной причиной аварий лишь в 20% случаев, тогда как к концу 80-х доля «человеческого фактора» стала близкой к 80%.

Одна из причин возникновения такой тенденции кроется в старом, традиционном подходе к построению сложных систем управления, т.е. ориентация на применение новейших технических и технологических достижений и недооценка необходимости построения эффективного человеко-машинного интерфейса, ориентированного на конкретного человека (диспетчера).

Таким образом, требование повышения надежности систем диспетчерского управления является одной из предпосылок к появлению нового подхода к разработке таких систем.

В конце XX – начале XXI века стали появляться работы с анализом реакций диспетчеров на те или иные нештатные ситуации. Мыслительный процесс диспетчера в процессе управления сложным объектом является процедурой, направленной на своевременное решение задач оценки состояния, диагностировании причин возникновения нештатных состояний и поиски соответствующих адекватных управляющих действий.

Поэтому последние десятилетия одним из ключевых направлений в разработке систем диспетчерского управления стало направление когнитивной графики и экологического интерфейса для помощи человеку-оператору в задачах оценки состояния сложной технической системы/объекта.

Как правило, системы диспетчерского управления включают в себя три уровня иерархии. На нижнем уровне располагаются датчики и исполнительные механизмы, на среднем – контроллеры, на верхнем – человеко-машинный интерфейс. Упомянутые выше направления когнитивной графики и экологического интерфейса применяют непосредственно при разработке верхнего уровня.

Следует, однако, отметить, что для решения ряда задач уместно дополнить когнитивной составляющей и нижний уровень. Так, например, это целесообразно в железнодорожной отрасли:

современный высокоскоростной железнодорожный транспорт предъявляет новые требования к организации мониторинга состояния объектов железнодорожной инфраструктуры, в особенности таких стратегических объектов как мосты, тоннели и т.п.

В работе рассматривается возможность переноса применения когнитивной составляющей на нижний уровень к датчикам, при этом каждый отдельный сенсор интерпретирует полученные данные как некоторый цвет (зеленый, желтый, красный, синий), а затем обменивается обработанной таким образом информацией с другими датчиками сети.

Такой подход позволяет в результате переговоров агентов-датчиков при помощи логических операций формировать целостную картину одного из контролируемых участков объекта.

Работа выполняется при финансовой поддержке РФФИ, проект № 14-07-31317.

Семенов А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова

ВЫЯВЛЕНИЕ ДЕМОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ВЫЯВЛЕНИЯ МУЗЫКАЛЬНЫХ ПРЕДПОЧТЕНИЙ

Определение скрытых характеристик пользователей на основе явно предоставляемой ими информации в социальных сетях и сервисах образует серию связных проблем, решение которых вносит вклад в множество прикладных областей от информационной безопасности до маркетинга. Одним из наименее исследованных предикторов являются музыкальные предпочтения индивида. Известно, что существует связь между ними и демографическими характеристиками.

В рамках настоящей работы мы исследуем возможность предсказывать пол и возраст пользователя сети vk.com на основе музыкальных композиций, размещенных у него на странице (в аудиозаписях и на стене).

Признаковое описание пользователя строится на основе вектора из хэштегов композиций, которые считываются для каждой музыкальной записи с портала last.fm.

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

ТЕСТИРОВАНИЕ ИНСТРУМЕНТАРИЯ ДЛЯ ОЦЕНИВАНИЯ ИНТЕНСИВНОСТИ УГРОЗООБРАЗУЮЩЕГО ПОВЕДЕНИЯ РЕСПОНДЕНТОВ

Одним из аспектов исследования безопасности информационной системы является изучение поведения пользователя, которое потенциально может создать угрозу защищенности этой системы. Предложен подход, позволяющий выполнять измерения интенсивности поведения на основе ответов респондентов о последних эпизодах того или иного вида угрозообразующего поведения. Однако, несмотря на то, что недавнее поведение (recent behavior) часто используется как показатель рискованности поведения, вопросы о том, в какой степени такие данные позволяют оценить интенсивность поведения, недостаточно изучены.

Для эффективного применения подхода на основе последних эпизодов при решении практических/прикладных задач необходимо не только получить численную оценку интенсивности, но и проверить, насколько сведения о последних эпизодах поведения позволяют характеризовать поведение в целом.

Для ответа на указанный вопрос исследовалось поведение в социальных сетях, для которого можно получить не только оценку на основе данных о последних эпизодах, но и фактические сведения о поведении за интересующий нас промежуток времени.

Разработано приложение, которое позволяет автоматически извлекать записи и комментарии к ним с пользовательской страницы социальной сети ВКонтакте. Проведено сравнение полученных оценок и фактических данных.

Разработанный инструментарий будет полезен при проведении различных исследований, одним из аспектов которых является изучение характеристик поведения.

Тишкина Н.В., Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России

СЕТЬ ИНТЕРНЕТ И ЗАШИТА ИНФОРМАЦИИ

Проблема защиты информации в глобальных компьютерных сетях актуальна как для государственных органов, так и для частных лиц и организаций, поскольку несанкционированный доступ внешних пользователей к какому-либо виду сервисного обслуживания, ввод в информационную систему вредоносного программного обеспечения, и другие несанкционированные манипуляции с информацией стали настоящим бедствием.

Работа в Интернет требует организации комплексной, многоуровневой системы защиты для всех субъектов.

Требования, направленные на обеспечение информационной безопасности:

– использование индивидуальных средств защиты на каждом компьютере,

– строгая регламентация и сертификация на соответствие требованиям информационной безопасности указанных средств,

– отказ от размещения в ЭВМ, которая подключена к Интернет, и в локальной сети, которая соединена с Интернет такой информации, несанкционированный доступ к которой может причинить ущерб интересам государства, личности, организации,

– организация работы с Интернет должна исключить возможность проникновения в базы данных локальных сетей, где циркулирует информация ограниченного доступа, включая государственную тайну и любую служебную информацию.

– разработка единых для всей России технических требований по оборудованию абонентских пунктов системы Интернет, которые были бы обязательны для государственных органов и организаций, а также для тех негосударственных структур, которые получили государственный заказ, в том числе оборонный.

– негосударственные структуры, коммерческие компьютерные сети, пользователи и провайдеры сети вправе самостоятельно решать вопросы обеспечения безопасности своих сетей, серверов и информации, если иное прямо не предусмотрено законодательством для конкретных случаев. Для провайдеров защита информации из права должна превращаться в обязанность, если на защите информации настаивает пользователь сети.

1. Распространение асоциальной информации, в том числе оскорбительных и непристойных материалов в сетях Интернет и доступ к ним несовершеннолетних;
2. Распространение недобросовестной (заведомо ложной) рекламы;
3. Различного рода мошеннические комбинации.

Основная проблема в сфере электронной коммерции – это проблема безопасности.

В электронном финансовом обороте не используются наличные денежные средства, поэтому участники Интернет-сделок должны быть уверены в том, что информация об их банковских счетах или номерах кредитных карт не будет получена какими-либо третьими лицам (за исключением операторов систем электронной торговли).

Преступления такого рода могут совершаться по следующей схеме: взламывается локальная сеть одного из виртуальных магазинов и переписывается программное обеспечение, включая пароли и бухгалтерские программы, соответственно у нарушителя появляется возможность отслеживать все операции покупателя, включая номер кредитной карточки. Прямо перевести деньги с одной кредитной карточки на другую нельзя, такая операция сразу становится заметной.

Поэтому, используя украденные пароли и программы, списываются деньги со счета покупателя на счет магазина, затем оформляется возврат от имени магазина не на счет покупателя, а на счет, который указывает виртуальный вор.

Сейчас система электронных платежей настолько громоздка, что большинство держателей кредитных карточек так и не узнают, что их обокрали.

4. Несанкционированный доступ к конфиденциальной информации.

Неправомерное вмешательство в частную жизнь гражданина посредством сети Интернет путем получения конфиденциальной информации либо путем несанкционированных публикаций его персональных данных возможно как со стороны частных лиц, так и со стороны государственных органов.

Торопова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СОЗДАНИЕ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ДИАГНОСТИКИ СОГЛАСОВАННОСТИ ДАННЫХ В МОДЕЛИ ОЦЕНКИ ИНТЕНСИВНОСТИ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ

Проблема диагностики согласованности данных встречается во многих задачах искусственного интеллекта. Многие модели и системы принятия решений строятся на основе экспертных методов, представляющих собой комплекс математически-статистических и логических методов и процедур, направленных на получение необходимой для подготовки и выбора рациональных решений информации от специалистов в исследуемой области.

В работе для решения проблемы диагностики согласованности данных в модели оценки интенсивности социально-значимого поведения используется аппарат байесовских сетей доверия.

Так как социально-значимое поведение может представлять собой активность пользователя в социальных сетях, полученные результаты можно использовать в том числе для решения задач социокомпьютинга.

Данный программный комплекс предназначен для расширения модели интенсивности социально-значимого поведения аппаратом диагностики согласованности данных респондента и вывода результатов этой диагностики в понятной для пользователя форме.

Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный университет

ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ В ЗАДАЧАХ СОЦИАЛЬНОГО КОМПЬЮТИНГА, СВЯЗАННЫХ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Одним из объектов изучения в области социального компьютинга являются сложные системы социотехнического характера, в частности, социальные сети, а также их подсистемы (группы по интересам, тематические чаты, аккаунты пользователей), комплексы «критичная информация – информационная система – персонал» (в том числе распределенные корпоративные компьютерные сети), системы электронных торгов, электронные магазины и т.д.

Эти системы обладают двумя общими чертами: 1) сетевой структурой, которая сама по себе может становиться средой, в которой развивается атака злоумышленника, имеющая целью достичь критичной информации и причинить вред (получить несанкционированный доступ, уничтожить, исказить, подменить, затруднить доступ санкционированным пользователям), либо иным образом нарушить функционирование системы; 2) социальной компонентой — пользователями, персоналом — которые сами по себе становятся либо «точкой» начала атаки злоумышленника, либо «средой», в которой такая атака развивается.

Для анализа, оценки вероятности возможности развития таких атак, оценки степени защищенности таких социотехнических систем требуется развивать комплекс математических моделей, в основе которого лежат вероятностные графические модели (байесовские сети доверия, алгебраические байесовские сети, марковские сети), а также модели, им родственные. Такие модели, с одной стороны позволяют с помощью достижений классической теории графов представлять структуру сложных социотехнических систем, а с другой стороны — учитывать недетерминизм поведения (реакции) пользователей в различных обстоятельствах за счет того, что узлами графов являются случайные элементы самой разной природы. Алгоритмы вероятностного и логико-вероятностного вывода, уже известные и использующиеся для обработки вероятностных графических моделей, как раз и открывают возможность получить искомые оценки различных аспектов защищенности социотехнических систем.

Тулупьева Т.В., Тафинцева А.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Северо-Западный институт управления РАНХиГС

СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК СВЕДЕНИЙ ДЛЯ ПОСТРОЕНИЯ ПСИХОЛОГИЧЕСКОГО ПОРТРЕТА

В современном мире трудно встретить человека, у которого не было бы страницы в социальной сети. Люди изо дня в день делятся своими мыслями, чувствами, событиями, интересами и фотографиями со своими друзьями, знакомыми и абсолютно посторонними людьми. В последнее время социальные сети используются не только как средство общения, но и для многих других целей, например как инструмент социального маркетинга или диагностики личностных особенностей. Насколько эффективно и перспективно использование социальных сетей в таких целях? Если страница в социальных сетях может дать информацию о личностных особенностях пользователя, то злоумышленник может использовать эту информацию для проведения социоинженерной атаки.

Было проведено пилотное исследование, нацеленное на выявление взаимосвязи между типами постов, которые пользователь размещает на своей странице Вконтакте, и его личностными особенностями, определенными при помощи психологических методик.

Исследование показало, что для пользователей, которые размещают информационные и эмоциональные посты самостоятельность не является жизненной ценностью. Побудительные посты размещают те, для кого важны самостоятельность и новизна в жизни. Поздравительные посты чаще публикуют люди, для кого ценность представляют традиции. Веселые, жизнерадостные, экспрессивные люди, а так же люди, придающие большое значение достижениям в жизни, наоборот, меньше размещают поздравительных постов. Посты с личной информацией о себе предпочитают размещать неуверенные в себе, обидчивые пользователи, для которых доброта является ценностью в жизни.

Проведенное пилотное исследование показало, что существуют взаимосвязи между предпочтением по размещению постов и личностными особенностями. Как следствие, злоумышленник, проанализировав посты на странице пользователя в социальной сети, может правильно подобрать атакующее воздействие и провести успешную социоинженерную атаку.

Тулупьева Т.В., Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук

СИСТЕМА КЛАССИФИКАЦИИ ПОСТОВ КАК ЭТАП ДИАГНОСТИКИ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Экспериментальные исследования молодежи показали, что респонденты демонстрируют поведение, при котором возможно снижение уровня безопасности информационной системы, в которой они работают. Другими словами, молодежь обладает высокой степенью уязвимости к действиям со стороны злоумышленника, направленным на получение конфиденциальной информации. В ряде работ был предложен подход к предсказанию таких уязвимостей через психологические особенности пользователя, однако вопрос быстрого (автоматизированного или автоматического) определения этих особенностей остается открытым.

Одним из этапов такого исследования является разработка классификации постов социальной сети, на основе которой затем можно делать выводы о личностных особенностях пользователя. В докладе описано приложение, реализующее систему классификации постов в социальной сети, основанную на автоматизированном выборе маркеров и обнаружении их в тексте. Предложенный подход предоставляет возможность для разработки нового инструментария для изучения личностных особенностей молодежи, что позволит разработать систему мониторинга, позволяющую своевременно начать профилактические или корректирующие мероприятия, направленные, в частности, на изменение поведения, приводящего к снижению уровня безопасности информационной системы.

Распространенность социальных сетей, их охват молодежи будет только увеличиваться, следовательно, исследование взаимосвязи между наполнением личных профилей (то есть тем, что и в какой форме публикуется владельцем аккаунта), ценностными ориентациями и степенью выраженности уязвимостей является актуальным на настоящий момент. Установление таких взаимосвязей может выступать как основа первичной экспресс-диагностики при работе с молодежью.

Федотова А.В., Бурдо Г.Б.
Россия, Москва, Московский государственный технический университет им. Н.Э.Баумана
Тверь, Тверской государственный технический университет

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ АСУТП ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

Выявление принципов создания интеллектуальных автоматизированных систем управления (АСУТП) дискретными технологическими процессами для разработки научно обоснованных методик создании автоматизированных систем управления технологическими процессами сборки и технического обслуживания высокотехнологичных изделий, в частности, является актуальной на сегодняшний день проблемой, востребованной Российской промышленностью.

Применение известных АСУТП технологическими процессами в многономенклатурном машиностроении затрудняется необходимостью корректировки планов всех уровней вследствие динамичной производственной ситуации, и постоянного появления новых контрактов.

Ситуация усугубляется для технологических процессов (ТП) с большой долей ручного труда, что приводит еще и к неопределенности времени выполнения неповторяющихся технологических операций. К таким технологическим процессам, в частности, относятся сборка изделий, техническое обслуживание изделий и их ремонт, изготовление новых образцов наукоёмкой продукции. В нашей работе рассмотрена АСУТП технического обслуживания авиационной техники, позволяющая минимизировать воздействие перечисленных выше негативных факторов. Кроме того, авторами предлагается вариант онтологического подхода к управлению знаниями и реализации онтологического инжиниринга применительно к одному из ключевых этапов жизненного цикла продукции - стадии ее технического обслуживания и ремонта.

Конкретная задача в рамках проблемы, на решение которой направлена работа - построение фундаментальных основ разработки интеллектуальной системы планирования и диспетчирования технологических процессов технического обслуживания с использованием технологий управления знаниями и онтологического моделирования.

В настоящей работе одно из центральных мест занимают онтологические методы структурирования и управления знаниями.

В докладе будут также представлены: общая классификация методов структурирования знаний применительно к ЖЦ авиационного оборудования, построеная система онтологий для обслуживания и ремонта авиационного оборудования, которая включает онтологию предметной области, онтологию задач, онтологию верхнего уровня; разработанные варианты гранулярного представления стадии технического обслуживания с различной степенью абстрактности, предложена модифицированная спиральная модель жизненного цикла с акцентом на стадию эксплуатации системы. Показано, что гранулярные примитивы (интервалы, распределения) имеют ключевое значение для онтологий жизненного цикла сложных технических систем.

В докладе будут представлены структура и модели интеллектуальной АСУТП ТО и ее модулей; показаны установленные принципы работы подсистемы объемного, календарного, оперативного планирования, а также подсистема диспетчирования, разработанные на основе приведенного выше математического аппарата. Реализация части моделей в АСУТП выполнена и на базе продукционных моделей знаний.

Федотова А.В., Давыденко И.Т., Святкина М.Н., Шункевич Д.В.
Россия, Москва, Московский государственный технический университет им.Н.Э.Баумана,
Республика Беларусь, Минск, Белорусский государственный университет информатики и радиоэлектроники

ОНТОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДЛЯ РЕАЛИЗАЦИИ СЕМАНТИЧЕСКИХ ТЕХНОЛОГИ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ

Настоящий доклад посвящен онтологическому подходу к построению систем управления жизненным циклом сложных технических систем. В данной работе проблема интеллектуализации управления ЖЦ сложной технической системы (СТС) рассматривается в контексте разработки систем управления жизненным циклом как системы управления знаниями, циркулирующими на всех этапах ЖЦ. В докладе будет представлена система, построенная по Технологии OSTIS. Архитектура интеллектуальной системы управления жизненным циклом имеет следующую структуру:

– база знаний системы – включает набор онтологий, описывающих предметные области, необходимые для организации процесса проектирования и совершенствования любой системы (Онтология Предметной области жизненного цикла систем, Онтология Предметной области деятельности, Онтология Предметной области технического обслуживания, Онтология Предметной области управления проектами и др.);

– машина обработки знаний системы – включает агенты, обеспечивающие поддержку деятельности исполнителей по развитию технической системы, управление задачами проектирования и сроками их исполнения и др.;

– пользовательский интерфейс системы– представляет собой подсистему, обеспечивающую взаимодействие пользователя с системой управления жизненным циклом технической системы.

Важнейшим аспектом управления знаниями на протяжении как всего ЖЦ СТС, так и его этапов является первоначальное структурирование знаний. К основным понятиям предметной области ЖЦ СТС относятся следующие: жизненный цикл системы, модель жизненного цикла системы, типовая модель жизненного цикла, модель жизненного цикла программного обеспечения, стадия жизненного цикла, техническое задание, эскизное проектирование, техническое проектирование, рабочее проектирование, технологическая подготовка производства и др.

Для формального описания знаний, касающихся управления проектированием интеллектуальных систем выделена Предметная область управления проектами. К основным ключевым понятиям данной предметной области относятся понятия проекта, продукта, проектной задачи.

В докладе будет рассмотрен подход к построению интеллектуальной системы управления жизненным циклом сложной технической системы. База знаний такой системы основана на системе онтологий предметных областей, обеспечивающих поддержку управления проектированием, а также дальнейшим совершенствованием сложной технической системы.

Федотова А.В., Ярушев С.А.
Россия, Москва, Московский государственный технический университет им.Н.Э.Баумана,
Международный университет природы, общества и человека «Дубна»

ГИБРИДНЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ

Прогнозирование представляет собой процесс составления проекций на будущее, основываясь на существующих исторических данных. Точный прогноз помогает в принятии решений и планировании на будущее, например, при планировании инвестиций или стратегий развития компании.

Среди множества методов, применяемых для прогнозирования, особое место занимают нейронные сети. Обусловлено это тем, что они способны выявлять сложно уловимые закономерности изменения временного ряда, а также рядом других достоинств, таких как способность работать в условиях недостаточности исторических данных, коротких временных рядов и нелинейности данных.

В условиях бурного развития знаний о структуре и работе мозга, всё большую популярность приобретают нейронные сети альтернативных архитектур.

В ряде проведенных нами исследований, были рассмотрены различные вариации архитектур, например, модульные нейронные сети, разработанные на основе работ Тетсуо Фурукавы. Такая модульная сеть представляет собой самоорганизующуюся карту, где нейроны заменены более сложными и самостоятельными структурами – отдельными нейронными сетями. Подобная сетевая архитектура позволяет повысить точность проноза и открывает большие перспективы применения в

задачах построения прогнозов, идентификации динамических объектов, в задачах информационной безопасности и управления.

В докладе также будут представлены наиболее известные на сегодня гибридные модели для прогнозирования временных рядов, их сравнение и качественная оценка. Особое внимание уделяется рассмотрению возможности гибридизации нейронных сетей и статистических методов прогнозирования.

Федотова А.В., Табаков В.В.
Россия, Москва, Московский государственный технический университет им. Н.Э. Баумана, Институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук

БОЛЬШИЕ ДАННЫЕ КАК ИНСТРУМЕНТ ПРЕОДОЛЕНИЯ ИНФОРМАЦИОННОГО БАРЬЕРА В СОЦИОКОМПЬЮТИНГЕ

Настоящий доклад посвящен анализу технологических особенностей понятия Больших Данных, как современной парадигмы реализации задачи обработки динамически растущих объемов информации в распределенных конвергентных информационных ландшафтах, примером которых является социокомпьютинг.

Общее ускорение процессов практически всех сфер жизнедеятельности вызывает лавинообразный рост объемов информации и повышение уровня сложности данных и способов их обработки. Таким образом, можно говорить о необходимости преодоления очередного информационного барьера и выходе за рамки изолированных замкнутых систем, поскольку, согласно закону теории информации, в изолированной системе информация может уменьшаться, либо оставаться постоянной, но не возрастать.

Под Большими Данными понимается группа технологий и методов производительной обработки динамически растущих объемов данных (структурированных и неструктурированных) в распределенных информационных системах, обеспечивающих получение качественно новой полезной информации, являющейся ключом к познанию. В цифровую эпоху человечество получило возможность проще и быстрее обрабатывать данные и мгновенно рассчитывать миллионы чисел. При этом вне зависимости от нашего стиля мышления Большие Данные диктуют три основных шага к новому образу восприятия данных. Первый – это способность анализировать все данные, а не довольствоваться их частью или статистическими выборками.Второй – готовность иметь дело с неупорядоченными данными в ущерб точности.Третий – изменение образа мыслей исследователя: доверять корреляциям, а не гнаться за труднодостижимой причинностью.

Современные подходы к обработке Больших Данных стремятся к совмещению целого ряда решений (суммы технологии) на базе единой интеграционной платформы, обладающей целостным единством (что, тем не менее, не подразумевает ее абсолютную универсальность!), и призванной решать сложнейшие задачи управления данными в конвергентных информационных средах в режиме реального времени. В докладе будут рассмотрены следующие технологии, составляющие ядро понятия Больших Данных: MapReduceиHadoop;NoSQLСУБД; СУБД с вертикальным хранением данных; In-Memory СУБД; Data Mining и прогнозная аналитика; Управление потоками событий. Особое внимание будет уделено Data Mining и прогнозной аналитике. Следует отметить, что отдельные технологии, способные в той или иной степени решать проблему фрагментации данных позволяют хранить огромные объемы информации, оперативно их обрабатывать, преодолевая информационный барьер. Однако основной вопрос применения технологии, как и ее ценность, заключается не в скорости обработки и передачи потоков данных в единицу времени, а в возможности формирования действительно репрезентативной выборки на основе генеральной совокупности данных, и последующем применении индуктивных методов для установления закономерностей и построении достоверных аналитических прогнозов. И в этом отношении Большие Данные решающим образом приходят на помощь науке, делая возможным, кроме алгоритмических вычислений – моделирование процессов с помощью таких инструментов, как генетические алгоритмы, нейронные сети и т.д.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-37-60004

ФлеровВ.Д., Эм П.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

СОЗДАНИЕ ЕДИНОЙ СИСТЕМЫ ДОСТУПА К СЕТИ ИНТЕРНЕТ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

На сегодняшний день безопасность в сети интернет является одной из основных проблем. В связи с этим возникает вопрос создание безопасного интернета на территории Российской Федерации. Так как многие пользователи используют ресурсы интернета в корыстных целях. В связи

с этим необходимо разработать методы, которые бы удовлетворяли условия по обеспечению безопасности в сети интернет на территории РФ.

Рассмотрим методы, которые используются на территории РФ.

1)Контроль за действием пользователей в сети интернет.

Данный метод основан на том, что каждый человек будет получать электронный паспорт в специально созданном государственном органе по типу паспортного стола. Где по достижению определенного возраста ему необходимо будет придти и зарегистрироваться для получение доступа к сети интернет, после чего ему будет выдан электронный паспорт, который храниться в базе данных системы. Для входа в сеть пользователь должен предоставить данные своего электронного паспорта, где будут указаны его идентификаторы. Подключение к ресурсам сети интернет будет осуществляться по возрастному показателю, то есть если возраст пользователя не соответствует возрасту, который указан на ресурсе то ему будет отказано в доступе. Сеансы клиентов будут контролироваться программными средствами, а выявленные подозрительные соединения - прерываться и анализироваться специалистами специального отдела.

2)Метод сбора данных и отслеживание статистики по трафику

Данный метод основан на том, что соединения пользователь будут записываться, храниться и обрабатываться в базе данных специального отдела. Соединения будут проверяться, и анализироваться специалистами специального отдела. При выявлении нарушений будут применяться правовые и организационные меры по решению данных нарушений. Данный метод позволит создать статистику о действиях пользователей в сети интернет и в дальнейшем разработать мероприятия по уменьшению нарушений в сети интернет.

3)Метод доступа к сети по гостевому профилю

Данный метод представляет собой процедуру идентификации, аутентификации при подключении к безопасному интернету на территории РФ. Каждому гражданину, находящемуся на территорию РФ необходимо, для подключения к сети интернет необходимо предоставить персональные данные. Система обрабатывает и анализирует информацию во время сессии пользователя.

Данные методы позволяют обрабатывать и анализировать данные при работе пользователей в сети интернет. Однако они не способны обеспечивать эффективную безопасность в сети интернет. Поэтому для решения данной проблемы необходимо подходить с точки зрения тотального контроля населения, однако законы РФ не позволяют осуществить данный метод. Вследствие чего необходимо разработать систему доступа к сети интернет, которая способна была обеспечивать комплексную защиту в сети.

Одно из решений в данной проблеме может быть создание единой системы, которая будет организовывать доступ к безопасному интернету. В данной системе будет организовано кредитная процедура для доступа в интернет. Она будет строиться по следующему принципу. На территории РФ необходимо будет создан федеральный орган по управлению доступа к сети интернет. Пользователь приобретает карточку, на которую должен положить денежную сумму, после чего он может получать доступ к сети интернет.

Фокин Р.Р.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОЙ МОБИЛЬНОСТИ

Образовательная мобильность рассматривается нами здесь в таком своем аспекте, как широкое применение обучаемыми и преподавателями мобильных технических средств. Это смартфон, планшетный компьютер, а также ноутбук, нетбук, ультрабук и т.п. Эти технические средства называют мобильными из-за их небольших размеров, веса, энергонезависимости, возможности для обучаемого и преподавателя пользоваться ими постоянно. Заметим, что данный аспект поддерживает образовательную мобильность в любом понимании этого термина, посколькумобильность – это подвижность, способность к быстрому изменению состояния, положения. Современный социокомпьютинг – это термин, описывающий многообразное использование и роль компьютерных технологий в современном обществе. Исходя из этого, широкое использование мобильных технических средств, гаджетов – это важнейшая черта современного социокомпьютинга. Сфера образования не должна ее игнорировать. При использовании методик обучения студентов с использованием мобильных технических средств нельзя обойти стороной вопросы такой актуальной ныне области знаний как информационная безопасность (ИБ). Подключение мобильного устройства в сеть, где присутствуют другие устройства, возможности которых (в частности – установленное там программное обеспечение и параметры его работы) по нарушению персональной ИБ студента или преподавателя заранее неизвестны. Определение подключаемой сети как общественной минимизирует ее функции, тем самым возможности мобильных устройств по обеспечению коммуникации между студентом и преподавателем или между студентами используются не

полностью. Так что проблему нельзя считать полностью решенной таким образом. Думается, проблема была бы решена в значительно большей степени путем корректировки политики ИБ вуза с учетом возможности обеспечения безопасных коммуникаций между мобильными устройствами.

Нетбуки, ультрабуки и планшеты за счет небольших размеров и веса относятся к компьютерам класса "всегда с собой". Эти устройства находятся всегда с собой у большинства современных преподавателей и студентов и готовы быть мощными инструментами в решении различных проблем, возникающих в процессе обучения информатике, тем самым являясь средствами разработки, применения и совершенствования различных скервисов обучения (СО). При этом нетбуки, ультрабуки и планшеты имеют свои достоинства и недостатки, которые и будут рассмотрены ниже.

Нетбуки в настоящее время являются самыми распространенными среди студентов и педагогов из-за очень низкой стоимости и высокого уровня функциональности. Они, как правило, оснащены емкими и дешевыми жесткими дисками и CISC-процессорами Intel Atom, с операционными системами (ОС) семейств Windows и Linux и, соответственно, с самым широким набором программного обеспечения (ПО). Недостатки: малая мощность процессоров не позволяет осуществлять такие операции, как нелинейный видеомонтаж (что большинству студентов и преподавателей не требуется), низкое качество и малый размер экранов способствуют ослаблению зрения. Ультрабуки значительно дороже нетбуков и в сфере образования их мало. Ультрабуки в отличие от нетбуков оснащены высококачественными экранами, мощными CISC-процессорами Intel i3, i5, i7, большинство их вместо жестких дисков (емких, дешевых, надежных, но медленных) оснащено флеш-памятью (малой емкости, дорогой, не надежной, но очень быстрой). Они имеют наибольшие перспективы для применения в сфере образования будущего. Для планшетов характерны высококачественные экраны. Класс планшетов с дополнительной съемной клавиатурой, с мощными CISC-процессорами Intel i3, i5, i7, с флеш-памятью большой емкости 128-256 Gb функционально от ультрабуков не отличается, аналогичны и перспективы применения в обучении информатике. Класс планшетов с экранами 7"-10", с RISC-процессорами сверхмалого энергопотребления, с ОС семейств iOS и Android пока имеют ПО, рассчитанное в основном на развлечения. Они дороги, но широко распространены среди студентов. Именно с появлением необходимого ПО связаны перспективы их применения в обучении информатике. Широкое применение мобильных технических средств, гаджетов обогатит современную педагогику как науку, сделает сферу образования в целом более эффективной. Использование настольных персональных компьютеров (ПК), которыми в учебные заведениясейчас обеспечены, не делает практически возможным создание и использование персонального информационного пространства ни преподавателя, ни тем более обучаемого. Мобильные ПК потребляют в десятки раз меньше электроэнергии. А если говорить омощности вредного высокочастотного электромагнитного излучения? А огромное количество компьютерных классов – это разве эффективное использование площади учебного заведения? В условиях ориентации сферы образования на мобильные ПК эти площади снова станут специализированными аудиториями для изучения географии, биологии, математики и т.п.

Эм П.С., Флеров В.Д.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

МЕТОДЫ БОРЬБЫ С ПОЛУЧАЕМОЙ В ИНТЕРНЕТЕ ЗАПРЕЩЁННОЙ ИНФОРМАЦИЕЙ С ПОМОЩЬЮ АНОНИМАЙЗЕРОВ

Сегодня все желающие взаимодействовать с запрещённой информацией могут довольно легко обойти законные запреты на доступ к заблокированным ресурсам с помощью сервисов, использующих технологии сохранения анонимности. Так как данная проблема является весьма острой не только в Российской Федерации, но и во всём мире, а методы эффективной борьбы с ней при текущих условиях использования Интернета применяются на практике без особого успеха, стоит рассмотреть более радикальные, затратные, но действенные методы.

1) Внедрение систем фильтрования трафика в существующие элементы сети. Возможно развитие таких технологий, как DPI(Deep Packet Inspection). Пакеты трафика, передающиеся по сети, будут изучаться системой на наличие подозрительного контента и, в случае обнаружения запрещённой информации, блокировать соединение клиента. Этот метод является для клиентов сети самым безобидным из представленных, но на сегодняшний день данная технология не позволяет запретить доступ к нежелательным ресурсам.

2) Разрешение доступа клиентам в Интернете только к проверенным ресурсам. Данный метод может помочь избавиться не только от возможности добывания запрещённой информации через сеть, но и закрыть доступ к нежелательным ресурсам. Владельцы сетевых ресурсов должны будут получить сертификат о внесении в реестр разрешённых сайтов у руководящей службы, а также должны быть предупреждены об определённой ответственности в случае нарушения условий

сертификации. Основным поводом для запрета будет наличие технологий анонимности и прямого/косвенного доступа к запрещённой информации.

3) Организация новой системы с использованием ПО и технических средств для создания сервиса, через который осуществляется доступ к Интернету на территории РФ. Данный сервис предполагает наличие у всех клиентов необходимых для авторизации в системе и доступе к Интернету идентификаторов личности. Сеансы клиентов будут фильтроваться программными средствами, а выявленные подозрительные соединения - прерываться и анализироваться специалистами специального отдела этого сервиса.

4) Создание национального аналога Интернета(новой сети объединения компьютеров) на территории РФ должно ограничить пользователей в возможности обходить запреты в сети с помощью различных способов туннелирования. Метод основан на физическом предотвращении доступа к ресурсам, которые могут содержать запрещённую информацию, а также постоянном контроле информации, циркулирующей в пределах сети, но при этом у обычных пользователей отсутствует связь с жителями других стран.

Каждый из этих методов может позволить эффективно разобраться с проблемой доступа к запрещённой информации, однако все перечисленные способы требуют огромных затрат. На реализацию самого дешевого метода из представленных уйдёт не менее 8 миллиардов рублей только на территории страны, что подводит к суждению о том, что обезопасить Интернет в ближайшие несколько лет без технологического прорыва не получится.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Балыкбаева У.А.,Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ПРИНЦИПЫ СООТНОШЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ И ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

Высокая профессиональная подготовка связана с непрерывным улучшением качества образовательных программ.

Системы управления качеством образовательных программ и системы сертификации взаимосвязаны с профессиональными стандартами. Профессиональный стандарт (ПС) является основой для проектирования образовательных стандартов и программ.

Анализ профессиональных стандартов ведущих стран позволяет спроектировать требования к содержанию и качеству образовательных программ, начиная от их разработки и до использования.

Метод анализа трудовых функций является самым эффективным при разработке ПС. При формировании ПС на основе метода анализа трудовых функций должен учитываться опыт успешных предприятий и компаний, международные тенденции развития определенной области профессиональной деятельности.

ПС разных стран существенно различаются и по структуре, и содержанию. Первая группа, где ПС описывают трудовые функции и входящие в них действия в рамках определенной профессии либо области профессиональной деятельности, а вторая где в ПСвключают дополнительные описания компетенций или перечень требуемых компетенций. В разрабатываемых проектах ПС сочетаются оба подхода.

Соответственно, связь профессиональных стандартов и квалификаций обеспечивается по-разному. В некоторых странах ПС разрабатываются отдельно и выполняют функцию классификации профессиональных областей. В другой группе стран разработка ПС интегрирована в процесс проектирования образовательных стандартов. В третью группу входят страны, где реализуется смешанная модель регулирования.

Опыт различных стран показывает, что тесная взаимосвязь требований сферы труда и системы образования приводит к организации профессиональной подготовки с целью придания ей определенной структуры и соблюдения последовательности прохождения учебных модулей. Существует задача на проектирование инструментов оценки, которые связывают требования сферы труда и их отражение в программах образования, соответственно и решаемая в разных странах по-разному.

При наличии профессиональных стандартов как отдельного документа, его трансформация в образовательный стандарт и стандарт оценки осуществляется в установленном в каждой стране порядке.

При проектировании образовательных программ различных уровней с учетом требований профессионального стандарта необходимо следовать единому набору принципов и единой методологии.

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ»

Наряду с позитивным влиянием на все стороны человеческой деятельности, широкое внедрение информационных технологий привело к появлению новых угроз безопасности людей. Это связано с тем обстоятельством, что информация, создаваемая, хранимая и обрабатываемая средствами вычислительной техники, стала определять действия большей части людей и технических систем, превратилась в очень дорогой товар. В связи с этим резко возросло количество предпосылок к нанесению ущерба, связанных с хищением информации, так как воздействовать на любую систему (социальную, биологическую или техническую) с целью ее уничтожения, снижения эффективности функционирования или воровства ее ресурсов (денег, товаров, оборудования)

возможно только в том случае, когда известна информация о ее структуре и принципах функционирования.

Вопросы информационной безопасности стали актуальными одновременно с появлением первых ЭВМ и совершенствовались совместно с развитием технической базы.

Массовое применение информационных систем в ряде областей человеческой деятельности (производственная, административная, технологическая, финансовая, патентная и др.), в которых информационное наполнение в большей степени не должно быть общедоступным, порождает новые проблемы и определяет возросшую актуальность защиты информации, содержащейся в продуктах интеллектуального труда.

На факультете информационных технологий Смольного института Российской академии образования в текущем учебном году в рамках рабочего учебного плана по направлению подготовки бакалавров 09.03.02 Информационные системы и технологии читается учебная дисциплина «Защита интеллектуальной собственности».

Целью дисциплины является формирование у студентов знаний по основам защиты интеллектуальной собственности, навыков и умения в применении знаний для конкретных условий.

В результате обучения студенты должны иметь представление об объектах интеллектуальной собственности, сформировать комплекс знаний о гражданско-правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации товаров, уметь выявлять нарушения авторского права, правильно лицензировать программное обеспеченье, составлять лицензионные договоры на разработанное ПО, регистрировать разработанные программы в различных фондах, составлять документы, входящие в состав заявки на получение патента на изобретение, полезную модель и промышленный образец.

Трудоемкость этой учебной дисциплины составляет 72 часа, из которых 18 часов – лекционных, 18 часов отведены для практических занятий. Она включает следующие основные разделы:

1. Информационная система как объект защиты.
2. Авторское право и его основные принципы.
3. Имущественные и личные права. Способы гражданско-правовой защиты.
4. Патентное право и его принципы.Объекты патентного права.
5. Источники патентной информации. Патентный поиск.
6. Охрана нетрадиционных объектов интеллектуальной собственности.
7. Виды правовой защиты интеллектуальной собственности.
8. Международное сотрудничество в сфере защиты интеллектуальной собственности.

Целью лекций является изложение нового теоретического материала и иллюстрация его примерами и задачами. Целью практической работы студентов является составление заявок на выдачу патентов и заявок на государственную регистрацию программы для электронных вычислительных машин или базы данных.

В помощь студентам при изучении этой учебной дисциплины автором написано учебное пособие «Защита интеллектуальной собственности», которое содержит новый актуальный материал по обеспечению защиты продуктов интеллектуального труда, а также составлены 6 практических заданий, помогающих в освоении лекционного материала и закреплении навыков составления документов по регистрации заявок на выдачу патентов, программы для электронных вычислительных машин или базы данных.

Башун В.В., Сергеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ЛИЧНЫЙ ЭЛЕКТРОННЫЙ КАБИНЕТ ПРЕПОДАВАТЕЛЯ КАК ВАЖНЫЙ ЭЛЕМЕНТ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ ПРОЗРАЧНОСТИ СОВРЕМЕННОГО ВУЗА

В соответствии с приказом Рособрнадзора от 29.05.2014 №785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети “Интернет” и формату предоставления на нем информации», вступают в силу новые требования к информации, размещаемой на официальном сайте ВУЗа. Новые требования приведены в п.3 приказа.

Согласно приказу, в Сети должна быть представлена информация о руководстве ВУЗа и персональном составе педагогических работников, в т.ч. преподаваемые дисциплины. По профессорско-преподавательскому составу должна быть представлена самая полная информация: личные данные, фотография, звание, степень, должность, место и время обучения, место и время повышения квалификации, ключевые публикации, патенты и другая информация.

Данное требование можно считать абсолютно обоснованным, т.к. со стороны студентов, партнеров и сотрудников ВУЗа имеется устойчивый спрос на информацию подобного рода: преподаватели и студенты нуждаются в общей площадке для обмена данными (например, выкладывания заданий и результатов тестов); при участии в конкурсах и составлении отчетности

нужна актуальная информация о публикациях и достижениях сотрудников;сотрудники нуждаются в объективной информации о компетенциях и возможностях коллег и т.д. Кроме того, наличие этих данных в публичном доступе является нормой для большинства зарубежных ВУЗов. И в любом случае наличие подобной информации в открытом доступе положительно сказывается на имидже учебного заведения.

С целью реализации требований Рособрнадзора, а также для увеличения информационной прозрачности и улучшения доступа к данным о преподавателях ВУЗа в ГУАП был разработан и введен в эксплуатацию веб-портал «Личный кабинет преподавателя». Создание портала, в конечном итоге, направлено на автоматизацию следующих процессов:

– Опубликование в глобальной сети базовой информации по профессорско-преподавательскому составу;

– Сбор информации о преподавателях, в том в числе по их научно-исследовательской деятельности;

– Сопровождение учебного процесса в части получения дополнительной информации по преподавателям;

– Сопровождение учебного процесса в части удаленного взаимодействия с преподавателем;

Система разработана с учетом обеспечения ее дальнейшего развития и наращивания функциональности. Ключевые требования:

– Масштабируемость. Система должна быть масштабируемой и расширяемой. При этом система должна быть устойчивой к увеличению количества авторизованных пользователей, посетителей и запросов, а также объема информации, хранимой в системе.

– Разграничение прав доступа пользователей к системе. Система должна поддерживать ролевую систему доступа, наличие различных ролей для доступа и работы в системе.

– Открытость. Система должна иметь открытые интерфейсы для взаимодействия и интеграции с другими системами.

– Многоплатформенность. В частности, не должно быть привязки к конкретной платной операционной системе, веб-серверу или СУБД.

– Ориентация на использование открытого, свободно-распространяемого программного обеспечения.

В настоящее время на портале представлена информация о всех преподавателях ВУЗа.

Бучкова Е.С., Быстрова О.Д., Федоров Д.Ю., Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ПЕРСПЕКТИВЫ РАЗРАБОТКИ И АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

В условиях научно-технического прогресса, активного развития производств и технологий, а так же динамично изменяющегося рынка труда, задача подготовки и отбора профессиональных кадров становится особенно актуальной и появляется необходимость создания и введения в практику новых, наиболее эффективных и реально работающих подходов и методов регулирования деятельности в данной сфере.

Увеличение темпов развития средств производства приводит к быстрому устареванию и обесцениванию полученных ранее профессиональных навыков, и требует их непрестанного и динамичного совершенствования. Нестабильная политическая обстановка в мире приводит к увеличению доли населения с различным, часто низким, уровнем образования.

В данный момент, профессиональные стандарты, имеющие широкое практическое применение за рубежом, рассматриваются как мощный инструмент, позволяющий создать прочное взаимодействие сфер труда и образования, обеспечивающий все условия для рационального использования человеческих ресурсов.

Для описания темыиспользуются понятия «квалификация работника» - уровень знаний, умений, профессиональных навыков и практического опыта работы, а так же «профессиональный стандарт» - характеристика квалификации, которая обязательна для работника, осуществляющего конкретный вид профессиональной деятельности.

Можно выявить несколько возможных положительных последствий введения профессиональных стандартов:

1) данные нормативные документы способны оказать помощь выпускникам школ в процессе профориентации – при выборе будущей профессии;

2) введение стандартов облегчит проведение профориентационной работы в соответствующих учреждениях и на курсах профориентации;

3) студентам высших учебных заведений будет легче определяться с направлением дальнейшей профессиональной деятельности;

4) унификация требований к навыкам и знаниям, а так же к уровню образования сотрудников.

На момент создания компетенций, отражающих навыки и умения, которыми должен обладать выпускник высшего учебного заведения, еще не были разработаны профессиональные стандарты. На наш взгляд, время обучения и сама учебная программа должны определяться компетенциями, выстроенными на базе трудовых стандартов.Если же трудовые стандарты будут разработаны в соответствии с уже имеющимися компетенциями, то, вполне возможно, уровень образования выпускников не будет соответствовать ожиданиям работодателей.

Необходимо, чтобы нынешние государственные федеральные стандарты образования соответствовали актуальным требованиям работодателей, представленных в форме профессиональных стандартов.

Разработка стандартов диктует необходимость соответствия международному уровню в данном направлении. База профессионального стандарта – опыт трудовой деятельности состоявшихся прогрессивных предприятий, которые являются лидирующими в своих отраслях.

Метод функционального анализа являет собой проведение опросов большого числа предприятий определенной отрасли, учет тенденций ее развития.

Разработка и введение стандартов немыслима без отбора и формирования групп экспертов, создания условий для их деятельности. Помощь специалистов понадобится и в самом процессе определения квалификации выпускников: на данный момент не ясно, кто именно должен будет заниматься проверкой компетентности студентов в их профессиональной области.

Возможно, появится потребность в создании отдельных компетентных органов, и появится необходимость в подборе штата практикующих специалистов. Перспектива переложить эти задачи на биржу труда не выглядит реальной – поток выпускников может парализовать ее работу. Возможно, стоит возложить ответственность на плечи работодателя, заинтересованного в рекрутинге юных специалистов.

В Российской Федерации ориентация сферы образования на потребности рынка труда находится на начальных этапах. Следует учитывать множество факторов, оказывающих влияние на ее развитие. Потребность в создании профессиональных стандартов ясна и требует участия всех сторон – системы образования, работодателей и обучающихся.

Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

РОЛЬ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСПЕКТЕ ЗАДАЧИ УЛУЧШЕНИЯ РОССИЙСКОЙ СИСТЕМЫ ОБРАЗОВАНИЯ

Причины разработки профессиональных стандартов многие правомерно связывают с недостатками образования в ВУЗах и, как следствие, с необходимостью контроля Министерством труда РФ приходящих кадров в службы занятости населения. Соответственно финансирование работ проводит указанное министерство и в настоящем году разрабатывается около 800 стандартов для различных специальностей, средней стоимостью 500 000 рублей каждый. При этом, целью стандартов является способствование решению такой основополагающей задачи, как уменьшение числа безработных. Каким образом профессиональный стандарт влияет на безработицу? В рамках стандарта упорядочиваются требования предприятий к работникам, занимающим конкретную должность, а, чтобы биржи труда могли, в свою очередь, для пришедшего к ним за помощью найти вакансию, эти должности связываются с конкретными специальностями профессионального образования. Пришедшему достаточно принести диплом, трудовую книжку, в которой указан его опыт, и какие-либо официальные документы, подтверждающие получение дополнительного образования, как тут же станет понятно, на какую должность он может претендовать. Данная схема математически точна и должна иметь прекрасный результат – безработица в стране среди людей, получивших какое-либо образование должна существенно уменьшится. К сожалению, весьма трудно опираться на официальную статистику для точного подсчета явных улучшений, но, по сути, приблизительную оценку можно выполнить следующим образом. Во-первых, биржи труда получают официальный запрос в основном от государственных бюджетных организаций, либо от крупных частных компаний и обеспеченных иностранным капиталом. Большая часть частного сектора, где поиск специалистов осуществляется путем расширения связей с профессиональной общественностью, охвачен не будет. Во-вторых, количество граждан, не сумевших попасть (или закончить) колледж или ВУЗ даже в таких крупных городах, как Санкт-Петербург составляет не меньше 10%, а по всей остальной стране количество таких людей существенно превышает официальные данные. В третьих, отсутствие работающих схем взаимосвязи между подразделений тех же государственных предприятий с собственными отделами кадров, связанное с постоянной экономической неопределенностью этих самых подразделений, тоже не позволит трудоустраивать специалистов, особенно высокого уровня подготовки. В результате, несмотря на наличие четких требований к знаниям, умениям и навыкам у Министерства труда к специалистам разных профессий, решение вопроса безработицы требует взаимосвязанных и дополнительных решений сложнейших задач государственного уровня.

В работе рассмотрены прогнозируемые затруднения и в части внедрения стандартов: отсутствие способов определения качества опыта, кроме как по количеству лет работы в области, отсутствие учета лиц, получивших аналогичное образование за рубежом, отсутствие привязки к действительным учебным программам и конкретным знаниям молодых специалистов после завершения обучения. Разработка стандартов под эгидой Министерства труда выполнена с учетом потребностей предприятий с возможностью корректировки в будущем учебных программ. Т.е. сегодня будут внедрены стандарты на биржах труда и только завтра, когда не найдется удовлетворяющих требованиям специалиста, будут скорректированы программы и спустя 5 лет появятся первые выпускники. Учитывая научно-технический прогресс есть высокая вероятность, что этого периода окажется достаточным для изменения требований у предприятий. Выпускники могут снова оказаться не у дел. Говоря в аспекте улучшения образования, необходимо вложение бюджетных средств в коррекцию имеющихся программ обучения специалистов (в т.ч. по защите информации) с привлечением к практике на предприятиях, начиная с первых курсов обучения, и субсидированием принимающих в образовательной программе организаций, путем, предоставления целевых работ, рассчитанных на силы обучающихся (т.е. с увеличенными сроками выполнения, более низкими требованиями к качеству, с пониженной ответственностью после внедрения результата наработки, пониженным налогообложением). Дополнительно в статье формулируется частная задача создания и предварительная структура защищенной информационной системы, позволяющей вводить данные как соискателю самостоятельно, так и работнику службы занятости, через веб-интерфейс с последующим выводом вакантных должностей из актуальной базы данных и возможностью электронного варианта формирования документов для последующего взаимодействия с потенциальным работодателем. Предусматривается стандартизированный вариант загрузки и обработки тестовых заданий в личном кабинете соискателя, ускоряющих процесс трудоустройства, а также определяющий непредвзятость работодателя.

Гаврилов Л.С.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ИНТЕРФЕЙС ДЛЯ МОБИЛЬНОЙ ВЕРСИИ ГРАФИЧЕСКОГО ПРИЛОЖЕНИЯ KRITA SKETCH

В настоящее время существует достаточно большое количество разных задач, которые попадают под определение «Компьютерная графика». Повсеместно в учебные планы школ и вузов вводится курс компьютерной графики. Существуют различные программы преподавания курса «Компьютерная графика» согласно направлению подготовки студентов.

Недостаточное развитие графических редакторов в предоставлении возможностей работы с графикой на планшетных ПК, сочетающих многофункциональность и тактильность без использования периферийных устройств, препятствует комфортной работе пользователя.

Существующие многофункциональные редакторы, как правило, не приспособлены для тактильной работы с ними. Таковы Adobe Photoshop, Corel Draw, Gimp. Кроме того, интерфейс указанных редакторов развивается достаточно медленно и не предоставляет комфортной работы без использования периферийных устройств.

Предлагаемый в докладе интерфейс используется пользователями планшетных ПК для работы с цифровой векторной и растровой графикой, разработанный редактор обладает интерфейсом, сочетающим возможность многофункциональной работы с графическими образами, а также с возможностью тактильной работы, рассмотрен подход к оперативному совершенствованию этого интерфейса при помощи специального конструктора.

Основой для разработанногопрограммного продукта служит редактор Krita Sketch. Технические параметры соответствуют редактору Krita Sketch. Существенному улучшению подвергается его интерфейс и внутренние компоненты, которые по функциональности соответствуют Adobe Photoshop, Corel Draw, Gimp, требующих для своей работы в десятки раз большего объема оперативной и дисковой памяти, и более мощных процессоров. Аналогично по стоимостным показателям: Adobe Photoshop, Corel Draw – десятки тысяч рублей за одну лицензионную копию, разработанный программный продукт – около тысячи рублей.

Графический редакторфункционирует на платформах Windows и Linux. Необходим CISC-процессор. В перспективе планируется сделать его многоплатформенным с использованием как CISC, так и RISC- процессоров.

ГейгерГ.В., МуллинаЭ.В., Радченко Н.В., Самойленко Е.А.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»

ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ВЗГЛЯД ДИПЛОМИРОВАННЫХ СПЕЦИАЛИСТОВ: АКТУАЛЬНОСТЬ, ПРАКТИЧНОСТЬ, ПЕРСПЕКТИВЫ

В процессе профессиональной деятельности подвергались изучению и анализу группа проектов профессиональных стандартов по направлению «Информационная безопасность».

Стандарт «Специалист по защите информации в автоматизированных системах» описывает пять видов деятельности: эксплуатации систем обеспечения информационной безопасности, обеспечении безопасности информации, разработки и реализации проектов по защите информации,контроль защищенности информации, а также управлении проектами по защите информации. В проекте стандарта тщательно сформированы трудовые и обобщенные трудовые функции, а также перечни предполагаемых должностей и пути должностного роста.

Проект стандарта по технической защите информации,представляет собой обширныйсписок трудовых функций, дающий работодателю и соискателю, представление о том какими знаниями, навыками и опытом должен обладать сотрудник претендующий на ту или иную должность. Проанализированы виды деятельности, указанные в стандарте по технической защите информации, такие как: проектирование объектов в защищенном исполнении, разработка систем и средств защиты информации, производство систем и средств защиты информации, эксплуатация систем и средств защиты информации, контроль защищенности информации, сертификационные испытания на соответствие требованиям по безопасности информации.

Разработанный стандарт оставляет задачу, требующую внимательного рассмотрения по учёту конкретных знаний, умений и навыков принимаемого на работу специалиста. В стандарте предусмотрено дополнительное обучение в объеме 72 часа, в действительности требующего большего внимания со стороны государства, так как отведенные стандартом часы регламентированы выделяемыми бюджетными средствами. Такой подход к повышению квалификации не дает гарантии, что соискатель будет обладать знаниями, необходимыми для работы по выбранному направлению, так как не известно каковы были его первоначальные знания после получения высшего образования по направлению «Информационная безопасность».

Рассмотрено описание структуры профессионального стандарта по информационно-аналитической деятельности в сфере безопасности, которая содержит в себе пять направлений деятельности. Освещается вопрос о необходимости разграничения понятий «Специалист по автоматизации информационно-аналитической деятельности» и «Специалист по информационно-аналитической деятельности в сфере безопасности», так как такие специалисты занимаются различными видами деятельности. Специалист по автоматизации информационно-аналитической деятельности занимается проектированием и созданием информационно-аналитической системы. В свою очередь, специалист по информационно-аналитической деятельности в сфере безопасности собирает, анализирует и обрабатывает информацию для получения общего состояния безопасности системы.

Необходимо учитывать не только опыт работы в сфере определенной деятельности, но и информацию, которая содержится в резюме соискателя. В трудовой книжке может быть указана конкретная должность, а навыки, отраженные в резюме, могут быть получены по другой сфере деятельности, включая ту, на которую в данный момент направлен работодатель.

Проект профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», который является основополагающим в линейке разрабатываемых стандартов. Даже поверхностный анализ представленных в проекте трудовых функций позволяет сделать вывод о многогранности и универсальности необходимых для знаний, навыков и умений. Анализ проекта стандарта дает представление, что такой подход к построение трудовых функций позволяет практически полностью охватить все направления обеспечения информационной безопасности, а также, точно регламентировать требования к профессиональным навыкам и умениям соискателей при приеме на работу. Однако, очевидной проблемой такого подхода является излишняя универсальность трудовых функций для данного направления, и как следствие, обучающимся по данной специальности потребуется значительное большое количество времени для достижения необходимой квалификации перед тем, как они смогут непосредственно приступить к выполнению своих трудовых функций.

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

ПРИМЕНЕНИЕ КОМПЬТЕРНОГО ОБУЧЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ни для кого не секрет, что сегодня компьютерное обучение переживает новый виток развития - появляются различные облачные сервисы, разрабатываются суперкомпьютеры, в основе которых лежат системы искусственного интеллекта (ИИ) - ярчайшим примером которого является IBM Watson. Помимо реальной технической пользы, данные разработки и технологии сильно популяризируют эту область и продвигают её в широкие массы.

Однако, если в каких-либо областях компьютерное обучение достаточно легко внедряется и начинает широко использоваться, то в области информационной безопасности (ИБ) не все так гладко.

В основе этой проблемы лежит то, что защита информационных систем (ИС) существует в большинстве случаев на основе статических правил обнаружения шаблонов атак. Такой подход уже давно достиг своего предела и самое время начать использовать компьютерное обучения для защиты ИС.

Переплетение ИИ и ИБ концентрируется, в основном, на анализе данных и их аналитике, то есть на чём-то гораздо большем, чем просто отчеты. Это дает возможность выявлять угрозы системе гораздо раньше, на этапе их появления, а не по факту взлома системы. За последние 10 лет атаки стали сложнее, а структура систем значительно расширилась. И дело далеко не в том, что получаемой информации для отражения угроз недостаточно - наоборот, существует переизбыток подобных данных, и время специалистов в области ИБ уходит на их обработку вместо того, чтобы делать шаги по устранению только лишь планируемой атаки на момент получения первых отчётов. Таким образом, автоматизированная обработка данных ИС сегодня - это ключ к повышению безопасности и устойчивости к различным угрозам.

Основной и, пожалуй, самой важной частью аналитики в контексте ИБ является аналитика пользовательского поведения. Основываясь на отчетах о поведении, большинство крупных взломов можно было бы избежать, так как все они имеют за собой одно сходство - кражу прав пользователей ИС, включая их администраторов. Следовательно, обнаружение различия в поведении пользователей системы и их сценариях - наиболее важный компонент преждевременного обнаружения угроз.

Для осуществления поведенческой аналитики необходимо знать кто является пользователем ИС. Системы идентификации и управления доступа помогают в разрешении вопроса о предоставлении информации для последующего вычисления оценки риска. Подобные системы также нуждаются в машинном обучении - они используют оценочную информацию, чтобы со временем становиться интеллектуальнее, изменяя свои правила со временем.

Примером такой системы можно назвать адаптивную аутентификацию (Risk Based Authentication), которая учитывает такие параметры как местоположение пользователя, устройство, IP-адрес и его историю, важность информации, к которой совершается доступ и другие параметры пользователя, для расчета оценки риска непосредственно перед тем, как предоставить пользователю доступ. Основываясь на этой оценке также можно производить пошаговую аутентификацию.

К сожалению, оценка самих рисков происходит по статическим правилам, а сложность настройки подобных систем может привести к тому, что оценка риска может быть просчитана неверно и пользователю будет предоставлен ошибочный доступ. Тем не менее, чем быстрее компьютерное обучение придет в область информационной безопасности, тем больше потенциальных угроз можно будет предотвратить.

Коваленко Д.И.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»

ОСОБЕННОСТИ НЕПРЕРЫВНОЙ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ОФИЦЕРСКОГО СОСТАВА ЭМС В СИСТЕМЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Выбор типов и количество кораблей с необходимым кадровым составом определяется Генеральным штабом МО РФ в соответствии с военной доктриной Российской Федерации. Всё это прямо или косвенно позволяет говорить о заказе Главным Штабом ВМФ подготовленных специалистов для имеемых и строящихся кораблей ВМФ.

В свете требований ГК ВМФ по подготовке высококлассных специалистов ВМФ, каждый военнослужащий в период прохождения военной службы должен повышать свой профессиональный уровень. В настоящее время эта задача решается так же и в стенах института дополнительного профессионального образования в системе индивидуальной непрерывной подготовки специалистов ВМФ.

Дополнительное профессиональное образование направлено на повышение уровня подготовки специалистов ЭМС перед назначением военнослужащих на должность и в ходе службы, не менее чем через 2 года после назначения на должность.

Учебные планы и программы этих групп составлены таким образом, что материал, преподающийся в ходе обучения на разных этапах подготовки, не повторяется.

Необходимым и достаточным условием успешного выполнения требований ГК ВМФ по обеспечению кораблей флота высококлассными специалистами, в частности ЭМС, основывается на согласованной работе заказчика (ГШ ВМФ), кадровых органов флотов и Военного Института ДПО.

Совместная работа ГШ ВМФ (заказчика) с кадровыми органами флота позволяет определить количество специалистов нуждающихся в повышении квалификации или переподготовке при смене сферы деятельности (количественный показатель), что в итоге позволяет повысить

профессиональный уровень военнослужащих на занимаемых должностях или подготовить их на замещение вакантных должностей.

Для конкретного определения должностей специалистов со своими функциональными обязанностями заказчиком (ГШ ВМФ) разработан «Единый квалификационный справочник» с функциональными обязанностями по каждой должности в ВМФ (качественный показатель подготавливаемого специалиста). Органами военного управления на основе «Единого квалификационного справочника» разработаны квалификационные требования, которые позволяют учебному заведению (ВИ ДПО) разработать учебные планы и программы на подготовку специалистов с качеством которое определил заказчик (ГШ ВМФ).

Высокий результат качества подготовки военных специалистов зависит не только от работы преподавательского состава, но и от подбора кандидатов на обучение, их мотивации в обучении, способности обучаться, уровня знаний и умений по занимаемым должностям. Поэтому кандидаты на обучение обязательно проходят профессиональный отбор (или входной контроль) на готовность пройти программу по занимаемой или вакантной должности.

Вариантов по прохождению входного контроля несколько. Первый вариант - проверка готовности кандидата по зачетному листу на самостоятельное управление подразделением. В идеале зачетные листы для кандидатов должны быть разработаны ОВУ по каждой должности и соответственно быть однообразными на всех флотах и флотилиях, но, к сожалению это пока не так. Комиссия, участвующая в выборе кандидатов на обучение определяет степень готовности кандидата к обучению или возвращает его на флот.

Вторым вариантом проверки готовности кандидатов к обучению, по занимаемой должности, является входной контроль по профессиональной пригодности, согласно квалификационных требований, разработанных заказчиком. При низком уровне ответов, кандидаты направляются обратно к месту службы.

Кандидаты на переподготовку для выполнения функциональных обязанностей в новой сфере деятельности проверяются по квалификационным требованиям соответствующим занимаемой должности и квалификационным требованиям должности, на которую кандидат должен будет готовиться.

Низкий уровень ответов, по занимаемой должности возвращает кандидата на флот. Результаты ответов по предстоящей должности позволяют произвести глубокий анализ готовности кандидата к обучению и разработать персональную, т.е. вариативную часть программы подготовки.

Формирование вариативной части программы подготовки военнослужащих проводится не только для тех, кто проходит отбор по квалификационным требованиям, но и тех, кто проходит отбор по зачетному листу на самостоятельное управление подразделением. На базе полученных результатов уровня подготовки специалистов ЭМС разрабатываются Учебные планы и программы, персонально на каждого прошедшего отбор кандидата.

На основании Учебных планов и программ персонально на каждого прошедшего отбор кандидата кафедрой разрабатываются тематические планы, сетевые графики, расписания занятий, т.е. учебно-методический комплекс. Таким образом, ВИ ДПО и кафедра готовиться к индивидуальной подготовке зачисленного кандидата.

В конце успешного обучения слушатели получают документы об окончании переподготовки или повышения квалификации. В дальнейшем планируется выдавать и сертификат о праве на выполнение обязанностей в должности, на которую проходили обучение.

Вернувшись на флот, после переподготовки и повышения квалификации на новую должность, выпускники в кратчайший срок сдают на допуск к самостоятельному управлению подразделением, с учетом особенностей проекта корабля (соединения кораблей). И в полном объеме приступают к выполнению своих обязанностей.

Проходя службу на флоте военнослужащие, в зависимости от срока нахождения в должности или уровня прохождения службы, по решению аттестационной комиссии направляется на повышение квалификации (по занимаемой должности), переподготовку для новой сферы деятельности или увольняется в запас, как не соответствующий занимаемой должности.

Лапин В.Н.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «FITNESS-КОНСУЛЬТАНТ»

В настоящее время большое количество людей самостоятельно занимаются укреплением здоровья, используя для этого системы физических упражнений и определенную диету. На первых порах у новичков возникает очень много вопросов. Лучше всего на них может ответить тренер, не только знающий свое дело, но и отлично знающий тренируемого, его индивидуальные особенности, всю историю тренировок. Если такого тренера нет, человек может тренироваться не оптимально, в каких-то случаях рискованно, часто испытывать дискомфорт от невозможности принять обоснованное решение, кроме того, вопросы часто возникают вне тренажерного зала, когда тренер недоступен.

Эту проблему может в значительной степени решить интеллектуальная программа, в которую заложены знания профессионального тренера по фитнесу, содержащая индивидуальные характеристики тренируемого, историю его тренировок, физического и психического состояния. Такой «тренер» всегда доступен, если его реализовать на мобильном устройстве.

Прямых аналогов разрабатываемого продукта не существует. Косвенные аналоги весьма распространены в таких интернет-магазинах как Play Маркет и AppStore, но они обладают значительно меньшей функциональностью, поскольку фактически используют только технологии интерактивного диалога с пользователем, но не технологии искусственного интеллекта.

Обсуждаемое в докладе приложение разрабатывается как экспертная система.

Вопрос об источнике знаний решается следующим образом. Сам разработчик активно занимается культуризмом, поэтому обладает определенным опытом и хорошо представляет себе трудности, возникающие у начинающих, кроме того всегда есть возможность проконсультироваться с опытными тренерами, имеется специальная литература.

Первоначально необходимо создать эффективную модель, позволяющую комплексировать знания по методам тренировки, спортивного питания и физиологии, так как система должна предлагать пользователю решения, отвечать на вопросы и, при необходимости, обосновывать свои рекомендации.

Важным источником знаний (опыта) является сам процесс эксплуатации приложения пользователями, так как все действия и полученные результаты фиксируются и накапливаются на сервере.

В архитектуре приложения как экспертной системы центральное место занимает база знаний, которая по структуре соответствует модели и отделена от кода (решателя), может независимо от него редактироваться, а при необходимости - использоваться другими приложениями.

Как мобильное приложение, программа строится по архитектуре «клиент — сервер». При этом вся функциональность, непосредственно интересующая конечного пользователя, реализована на клиенте.

В ходе работы вся история тренировочного процесса сохраняется, что является важным условием для выработки экспертных решений (рекомендаций системы). На случай порчи данных, смены или выхода из строя мобильного устройства вся необходимая для работы приложения информация дублируется на сервере.

Накапливающаяся статистика тренировок является важным источником информации для усовершенствования базы знаний экспертной системы. Таким образом, имеются:

1) клиент - «фитнесмен» - конечный пользователь приложения;

2) клиент - «эксперт», который берет данные с сервера, дорабатывает базу знаний и реализует это в виде обновлений системы;

3) сервер, служащий для хранения данных.

В настоящее время разработана архитектура программы как экспертной системы и как мобильного приложения. Программно реализован макет программы. Принципиально решены вопросы обеспечения информационной безопасности.

Первый релиз планируется осуществить на платформе Android. Разработка ведется средствами Android Studio. Базовый язык программирования — Jawa, при необходимости могут использоваться и другие языки.

Подружкина Т.А., Федоров Д.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербургский государственный экономический университет

ПРОБЛЕМНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СТАНДАРТИЗАЦИИ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Ускорение темпов технологического развития общества привело к существенному отставанию высшего образования от возрастающих требований рынка, как в области информационных технологий, так и в области информационной безопасности (ИБ). Рассмотрим возможности преодоления обозначенного разрыва в условиях нарождающейся стандартизации профессиональной деятельности, для чего составим «идеальную» схему подготовки специалиста в области ИБ, в которой принимают участие все заинтересованные субъекты.

Работодатель (представитель рынка) структурирует профессиональную деятельность специалиста по ИБ, формируя перечень трудовых функций и критерии их выполнения, а также формулирует требования к его знаниям, умениям, навыкам и компетенциям (ЗУНиК). Эти требования служат руководством для составления образовательных программ и стандартов, которые в свою очередь влияют на учебные планы и рабочие программы вузов. После этого происходит непосредственно процесс обучения, на выходе которого получается бакалавр (специалист) с набором ЗУНиК, коррелирующих с требованиями рынка. Затем, чтобы подтвердить свою квалификацию, выпускник может в независимом центре пройти процедуру сертификации на соответствие

определенному уровню квалификации и после этого смело идти устраиваться на работу. Контур замкнулся.

В реальности дело обстоит несколько иначе. Работодатель (рынок ИБ) нуждается в квалифицированных кадрах, которые бы приносили доход компании. Обеспечить компании кадрами – цель подготовки специалистов ИБ. По различным оценкам в стране не хватает от 4,5 тыс. до 20 тыс. специалистов. Сложности возникают уже при попытке собрать и формализовать огромный разброс ЗУНиК из должностных инструкций или опыта сотрудников на местах. Компании не заинтересованы своими силами (за счет времени сотрудников) предоставлять требования к ЗУНиК для формирования профессиональных стандартов. Отсюда получается, что профессиональные стандарты содержат лишь срез ЗУНиК, требуемых на рынке.

Излишне говорить, что сама процедура их получения неформализована и потому в принципе не автоматизируема и не верифицируема. Сегодня она выглядит следующим образом: в первую очередь, организация-разработчик совместно с экспертами изучают вид профессиональной деятельности (прогнозируемые изменения, возможности профессионального развития и т.д.), затем анализируются трудовые функции и проектируется функциональная карта. Полученный проект функциональной карты является основой для разработки анкеты, необходимой для проведения опроса работодателей и профессионалов отрасли. По результатам опроса в функциональную карту вносятся изменения, т.е. удаляются из функциональной карты функции, важность которых признана низкой большинством опрошенных. Таким образом, технология разработки профессиональных стандартов экстенсивна: чем больше стандартов, тем больше экспертов, и больше обсуждений, тем совершеннее (по мнению авторов подхода) должен быть разработанный стандарт.

Перейдем к образовательному стандарту. Текущие стандарты по направлению ИБ содержат собственный набор ЗУНиК, который не вытекает из ЗУНиК профессиональных стандартов, т.к. разрабатывались раньше и потому независимо. Более того: реалии сегодняшнего состояния дел таковы, что в стандарты деятельности перекачиваются ЗУНиК из образовательных стандартов единым разработчиком.

На выходе схемы подготовки получаем реального выпускника, который в течение 4-5 лет изучал дисциплины учебного плана, преподаваемые по большей части теоретиками (10% практиков погоды не делают), и приобрел свой собственный набор ЗУНиК. Не трудно догадаться, что этот набор сильно отличается от заявленного в стандартах или декларированного на бумаге (в дипломе).

Подтвердить полученные ЗУНиК выпускник мог бы, пройдя процедуру сертификации по примеру зарубежных CISA, CISM или CISSP. На данном этапе можно было бы проводить проверку, опираясь на профессиональные стандарты. Организация подобных центров могла бы существенно снизить нагрузку компаний на переобучение поступающих кадров, т.к. происходил бы отсев по наличию у соискателя сертификата. Проблема в том, что подобные центры еще не созданы.

Таким образом, реальная схема подготовки специалиста ИБ далеко отстает от идеальной и напоминает игру в «испорченный телефон»: у каждого субъекта цепочки собственный набор ЗУНиК; при переходе к следующему шагу этот набор искажается и передается дальше; отсюда получаем, что на выходе ЗУНиК бакалавра (специалиста) не соответствуют реалиям рынка. Обозначенная схема с обратной связью замыкается при прохождении всей цепочки, т.е. контроль происходит каждые 4-5 лет – это большой период с учетом стремительного развития информационных технологий, который требует сокращения и корректировки на каждом шаге процесса подготовки специалиста по ИБ.

Пригода А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

БИБЛИОТЕКА ПРОГРАММНЫХ ГРАФИЧЕСКИХ МОДУЛЕЙ ДЛЯ РАЗРАБОТКИ САЙТОВ МАЛЫХ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ

Разработка веб-сайтов крупных коммерческих компаний, как правило, требует не только применения веб-редакторов и CMS, но и значительных усилий веб-программистов и дизайнеров. В этом случае наибольшая доля стоимости разработки веб-сайта приходится именно на веб-программирование и дизайн. Малые коммерческие предприятия не могут себе этого позволить.

Существующие веб-редакторы и CMS системы, включая CMS 1С-Битрикс имеют ограниченную функциональность, не позволяющую полностью использовать возможности современных графических технологий.

В связи с санкциями США и ЕС по отношению к Российской Федерации вероятно появление проблем с использованием инструментального программного обеспечения иностранных разработчиков. Разработанный отечественной программный продукт будет способствовать решению этих проблем.

Предлагаемая библиотека программных графических модулей позволяет многократно снизить стоимость разработки качественного веб-сайта малого коммерческого предприятия.

В докладе рассмотрены вопросы классификации web-сайтов, этапы разработки, приводится анализ программных средств.

Предлагаемое программное обеспечение является многоплатформенным. Со стороны сервера могут использоваться любые современные интернет-серверы, такие как Apache, Microsoft IIS и др. Со стороны клиента могут использоваться наиболее известные интернет-браузеры, такие как Microsoft Internet Explorer, Opera, Google Chrome, Mozila и др.

Рожкова В.Е.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ АВТОМАТИЗАЦИИ РАБОТ ДЕКАНАТОВ И КАФЕДР ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

В настоящее время в российских вузах применяются различные программные средства, каждое из которых выполняет, как правило, какую-нибудь одну локальную функцию автоматизации работы подразделения. Комплексной автоматизации при этом не происходит.

Для обеспечения комплексной автоматизации необходимо предварительное изучение работы соответствующих подразделений с использованием методов и технологий реинжиниринга. Эти методы основаны на CASE-технологиях с использованием языков моделирования iDef и UML.

Целью выполнения работы является разработка программного продукта, служащего для повышения эффективности и качества работы сотрудников кафедр и деканатов высших учебных заведений.

Программный продукт автоматизирует процессы управления деканатами и кафедрами в высших учебных заведениях. Этот продукт значительно сокращает время реализации определенной задачи, поставленной перед сотрудниками.

При разработке программного продукта был предложен новый алгоритм, позволяющий существенно повысить эффективность и качество работы.

Создание самого программного продукта реализации информационных технологий управления выполняется на языке программирования высокого уровня С с применением языка моделирования UML.

Разрабатываемый программный продукт комплексно реализовывает большое количество функций управления. Этим он напоминает ERP-системы управления предприятиями. Среди известных ERP-систем можно назвать 1С:Управление предприятием, Галактика, Microsoft Dynamics Nav.

Конечный программный продукт функционирует на платформе Windows. В перспективе предполагается разработка многоплатформенной сетевой распределенной системы.

Потребителями разработанного программного продукта являются деканаты и кафедры отечественных вузов.

Сергеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

УЧЕБНЫЙ КУРС ПО РАЗРАБОТКЕ ВСТРАИВАЕМЫХ СИСТЕМ НА БАЗЕ МИКРО-ПЛАТФОРМ INTEL

Встраиваемые устройства в настоящее время используются в системах связи, на транспорте, в космических и авиационных системах, в управлении производством. Особенно широко они нашли своё применение в различных системах безопасности: контроле доступа, системах регистрации и т.п. Особенностями таких систем являются минимальное энергопотребление, наличие специализированного микропроцессора, минимальные габариты и вес, отсутствие специальных схем охлаждения, надежность и т.п. Аппаратной базой для построения встраиваемых устройств являются одноплатные микро-компьютеры, микроконтроллеры, системы-на-кристалле, специализированные или универсальные микропроцессоры, ПЛИС.

В связи с этим, остро стоит вопрос о подготовке студентов работе с данным классом систем. Увы, его решение затруднено целым рядом объективных причин. Во-первых, встраиваемые устройства обладают узкой специализацией устройств и своей спецификой программирования. Ограниченность учебных часов не позволяет изучить в рамках учебного курса специализированный язык программирования (даже относительно простой как Arduino). Во-вторых, узкая специализация встраиваемых аппаратных платформ не способствует переносу навыков, полученных на одном устройстве, на другие устройства. В-третьих, стоит сказать про острую нехватку квалифицированных преподавателей, обладающих опытом программирования и использования данных устройств.

Описанные проблемы могут быть решены созданием учебного курса, который:

– опирается на аппаратные платформы широкого назначения, а не на узко специализированные;

– не требует изучения нового языка программирования;

– позволяет легко продемонстрировать возможности встраиваемых систем: работу с датчиками, высокую автономность работы от аккумуляторных батарей, возможность удаленного управления другими объектами и т.п.

– использует недорогие устройства, свободно доступные на рынке;

– имеет низкий уровень профессионального вхождения.

Такой учебный курс был разработан в СПбГУАП для студентов, обучающихся по направлению «Информационная безопасность». Он опирается на новейшие встраиваемые x86-совместимые микро-платформы корпорации Intel на базе процессоров IntelQuark и IntelAtom.

Новейшие аппаратные платформы Intel, обладая всеми характеристиками встраиваемых устройств по энергопотреблению и массо-габаритным характеристикам, значительно превосходят последние по производительности и по стоимости на логическую операцию. Используемая x86-архитектура позволяет использовать на устройствах Linux-совместимые операционные системы, что значительно упрощает процесс создания программного обеспечения.

В настоящее время корпорация Intel создала полную экосистему подобных устройств: IntelGalileo как дешевое устройство для массового первоначального обучения, IntelEdisonArduinoBoard как платформа более высокого уровня, IntelEdisonBreakoutBoard для конечных технических решений и прототипирования. Все платформы могут работать со стандартными датчиками Arduino.

Учебный курс включает учебные материалы (в форме презентаций и сопроводительного текста), программные примеры (в виде исходного кода с пояснениями) и шаблон учебно-демонстрационного стенда для решения задачи организации защищенной шифрованной видео трансляции с встраиваемого устройства в вычислительное облако с последующей пост-обработкой (детектирование объектов, улучшение качества и т.п.). Подобный сценарий использования встраиваемых систем используется в системах контроля доступа, удаленного мониторинга, удаленного зондирования земли и т.п. Рассматриваемый в курсе сценарий облачной обработки видео полностью соответствует концепции IoT, когда вычислительно сложные операции вынесены в удаленное вычислительное облако.

Курс демонстрирует широкие возможности совместной интерактивной работы подсистем передачи видео и подсистемы сенсоров, установленных на встраиваемых устройствах (включение/выключение камеры по событию от датчиков, изменение режимов работы камеры в зависимости от сенсорной информации и т.п.).

В качестве языка программирования в рамках курса могут использоваться C/C++ (полномасштабный курс) или Python (упрощенный вариант), а такжеоперационная системаLinux.

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

ПОДГОТОВКА КАДРОВ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В РАМКАХ ФЕДЕРАЛЬНЫХ ГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТОВ ЧЕТВЕРТОГО ПОКОЛЕНИЯ

Переход кразрабатываемым в настоящее время федеральным государственнымобразовательным стандартам (ФГОС) четвертого поколения отражает тенденцию дальнейшего сближения Российской высшей школы с мировой образовательной системой и рассматривается как очередной шаг к сближению высшего образования и рынка труда. При этом следует ожидать большей корреляции направлений подготовки кадров по широкому спектру потребностей рынка труда в специалистах - разработчиках информационных систем и технологий, что требует серьезной проработки как наименований укрупненных групп направлений и специальностей, так и содержания подготовки.

Отличительными особенностями построения ФГОС четвертого поколения являются: преемственность образовательных программ,их дальнейшая интеграция с ориентацией на укрупненные группы направлений и специальностей, привязка к сопряженным профессиональным стандартам, расширение самостоятельности образовательных организаций в формировании образовательного процесса, возрастание ответственности за его результаты.

С одной стороны, это потребует глубокого анализа содержания профессиональной деятельности выпускников, требований к структуре, условиям реализации и результатам освоения основных профессиональных образовательных программ, структуры и содержания формируемых компетенции. С другой стороны, это накладывает большую ответственность на разрабатываемое учебно-методическое обеспечение подготовки кадров по входящим в укрупненные группы направлениям подготовки бакалавров и магистров и как следствие -обуславливает возрастание роли учебно-методических объединений и научно-методических советов высшей школы.

Идеология построения основных образовательных программ разработчиков информационных систем и технологий в рамках ФГОС3+ предусматривала исключение из планов подготовки бакалавра 09.0.02 и магистра 09.04.02 базовой дисциплины «Информационная безопасность и защита информации» как самостоятельной и интеграцию ее содержания во все ключевые дисциплины блока базовых дисциплин, изучающих методы и средства проектирования информационных систем, модели объектов и процессов информационных систем, технологии обработки данных и т.п.

При переходе к ФГОС 4 поколения интеграция существующих направлений подготовки бакалавра и магистра заставляет усилить базовую фундаментальную подготовку. В связи с этим на новом эволюционном витке особую актуальность приобретает базовая дисциплина«Информационная безопасность и защита информации», которая должна заложить основы знаний у студентов как в области защиты информации, так и в области защиты от информации.

Особое внимание должно быть уделено актуализации содержания обсуждаемого сегмента ФГОС с существующими и разрабатываемыми в настоящее время профессиональными стандартами в области информационной безопасности и защиты информации.

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

АКТУАЛИЗАЦИЯ ФГОС ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В РАМКАХ ПРОФИЛЯ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Совпадение по времени разработки профессиональных стандартов в области информационной безопасности и защиты информации и федеральных государственных образовательных стандартов (ФГОС) четвертого поколения дает уникальную возможность системной увязкисодержания подготовки и формируемых компетенций с требованиями рынка труда к профессиям и трудовым функциям, к выполнению которых должен быть готов выпускник.

В настоящее время возникла серьезная проблема трудоустройства бакалавров ввиду несоответствия их квалификации требованиям работодателей к конкретным рабочим местам. В итоге подавляющая часть выпускников испытывает трудности, связанные с трудоустройством: более 20% меняют место работы в первый год после окончания вуза.

Чтобы разрешить эту проблему, разработчиками ФГОС на основе анализа видов профессиональной деятельности, видов экономической деятельности и трудовых функцийна конкретных рабочих местах проведено согласование ФГОС с утвержденными профессиональными стандартами в двух направлениях, связанных с определением профессий, на которые может претендовать выпускник с соответствующей квалификацией, и определением обобщенных трудовых функций, выполняемых выпускником на конкретных рабочих местах.

Были подготовлены предложения Министерству образования и науки РФ о внесении изменений в ФГОС высшего образования в части учета положений профессиональных стандартов дляконкретных профессий и указания конкретных обобщенных трудовых функций, на освоение которых направлены программыбакалавриата и магистратуры.

В частности, вФГОС по направлению подготовки бакалавра 09.03.02 должны быть учтены требования 11 сопряженных профессиональных стандартов, вФГОС по направлениюподготовки магистра 09.04.02 -8 профессиональныхстандартов.При этом определено, что программабакалавриата 09.03.02 должна быть направлена на освоение 16 обобщенных трудовых функций, а программа магистратуры 09.04.02 -11 обобщенных трудовых функций.

Результаты проведенного анализапрофессий и обобщенных трудовых функций, сопряженных с профилем подготовки бакалавра «Безопасность информационных систем», позволили сформулировать требования к основной профессиональной образовательной программе и, в частности, к содержанию дисциплины «Информационная безопасность и защита информации», что представляет важным в условиях интеграциинаправления09.03.02 с другими направлениями подготовки бакалавра и привязкой ФГОС 4 поколенияк укрупненнойгруппе направлений.

Результатом явилось формирование новых актуализированных ФГОС, которые могут рассматриваться в качестве основы при разработке ФГОС четвертого поколения.

Дальнейшее развитие этого процесса должно привести к определению весовых оценок работы выпускниковпо той или иной профессии и реализации соответствующих обобщенных трудовых функций бакалаврами и магистрами после окончания вуза.

Опыт реализации ФГОС позволяет сформулировать рекомендации по дальнейшему сближению квалификации выпускников и потребностей работодателей.

Вместо актуализации ФГОС как вынужденного подхода на современном этапе, предлагается пойти по пути гармонизации, основанной на реализацииклассическойпоследовательности: «требования работодателей → профессиональные стандарты →компетенции →ФГОС».

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РАМКАХ ПОДГОТОВКИ БАКАЛАВРОВ И МАГИСТРОВ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Построение эффективной информационной системы не возможно без учета проблемы информационной безопасности на всех стадиях жизненного цикла от процесса проектирования до эксплуатации. Сложившийся в настоящее время подход к обеспечению информационной безопасности на стадии готового проекта информационной системы является недостаточно эффективным как с позиций технических, так и экономических.

Требования к уровню защиты конфиденциальных данных формулируются заказчиком на стадии разработки технического задания и реализуются в процессе проектирования и внедрения системы, а не на стадии конечного продукта. Это обеспечивает достижение требуемых характеристик проектируемой системы и оптимальное использование ресурсов – финансовых, материальных и трудовых.

При создании сложных, распределенных информационных систем, формировании их архитектуры, выборе компонент и связей между ними, требования к безопасности следует учитывать наряду с требованиями надежности, эргономики, обслуживания и т. д. Информационная безопасность должна обеспечиваться с учетом стандартов ISO/IEC, ANSI/IEEE на всех стадиях жизненного цикла информационных систем от разработки технического задания

Подход к учету информационной безопасности реализован для бакалавров в виде учебного блока, включающего дисциплины «Методы и средства проектирования информационных систем», «Корпоративные информационно-управляющие системы» и междисциплинарного проекта «Проектирование корпоративно-управляющей системы». Для магистров учебный блок включает дисциплины «Модели объектов и процессов информационных систем», «Современные методы и средства проектирования информационных систем», «Технологии распределенной обработки данных», междисциплинарного проекта «Разработка (исследование, проектирование) сложной информационной системы».

Такая постановка задачи обучения дает наглядное представление студенту о том, что проектирование информационных систем является коллективным процессом и все члены коллектива, включая специалистов в области информационной безопасности, участвуют во всех стадиях создания конечного продукта. Этим достигается решение важной проблемы обеспечения высоких показателей проектируемой информационной системы:

– обеспечение целостности, доступности, конфиденциальностикомпонентинформационной системы;

– гарантия непрерывности и корректности функционированияинформационной системы;

– длительный жизненный цикл информационной системы с множеством базовых и пользовательских версий;

– гибкость модификации и обеспечение информационной безопасности при развитииинформационной системы;

– унификация и стандартизация проектных решений, включая информационную безопасность.

Необходимо повторить, что высокое качество информационных систем достигается при определенных совокупных затратах ресурсов – финансовых, материальных и трудовых, на разработку этих систем.

Усольцев А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования

БИБЛИОТЕКА ПРОГРАММНЫХ МОДУЛЕЙ РАСШИРЕНИЯ ФУНКЦИЙ CMS 1С-БИТРИКС И МЕТОДИКА РАЗРАБОТКИ САЙТОВ МАЛЫХ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ

Существующие CMS системы, включая CMS 1С-Битрикс имеют ограниченную функциональность, не позволяющую полностью использовать возможности современных веб-технологий.

Разработка веб-сайтов крупных коммерческих компаний, как правило, требует не только применения CMS, но и значительных усилий веб-программистов. В этом случае наибольшая доля стоимости разработки веб-сайта приходится именно на веб-программирование. Малые коммерческие предприятия не могут себе этого позволить.

В связи с санкциями США и ЕС по отношению к Российской Федерации вероятно появление проблем с использованием инструментального программного обеспечения иностранных разработчиков.

В докладе рассмотрены современные подходы и программные средства создания сайтов, в частности,язык гипертекстовой разметки HTML; язык таблицы каскадных стилей CSS; скриптовый

язык программирования JavaScript; Flash-технологии, скриптовый язык PHP; система управления базами реляционными данных MySQL.

Детально рассматривается навигация и система управления сайтом. Навигация по сайту построена таким образом, что все блоки соединены между собой и при необходимости имеется возможность перехода с одного блока на другой.

Обсуждаются проблемы тестирования готового программного продукта.

Предлагаемое программное обеспечение является многоплатформенным. Со стороны сервера могут использоваться любые современные интернет-серверы, такие как Apache, Microsoft IIS и др.

Со стороны клиента могут использоваться наиболее известные интернет-браузеры, такие как Microsoft Internet Explorer, Opera, Google Chrome, Mozila и др.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Абакумов А.А. , Сорокин И.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

УЛУЧШЕНИЕ МЕТОДА РАСПОЗНАВАНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНЫХ ДОМЕННЫХ ИМЕН В СЕТИ ИНТЕРНЕТ

Некоторые разновидности вредоносных программ используют алгоритмы генерирования доменных имен для определения адресов управляющих серверов. Алгоритмы генерации доменных имен (DGA) часто используются при создании ботсетей. Это позволяет удерживать контроль над управляющими серверами. В основном подобные алгоритмы используются в крупных ботсетях. Для обнаружения вредоносных доменных имен удобно использовать алгоритмы машинного обучения. Возможность их использования подтверждают тезисы, выдвинутые на Конгрессе Молодых Ученых (2015г.). Однако были принято решение по улучшению предложенного метода. Поэтому целью работы является улучшение метода и его апробация.

Метод. Для тестирования была составлена обучающая выборка. Выборка состоит из 2 классов. Первый - Legit, был взят из списка Alexa Top Million. Второй - DGA, был составлен путем обратной разработки алгоритмов генерации вредоносных доменных имен, взятых из экземпляров вредоносных программ, существующих в сети Интернет. Не секрет, что зачастую самым важным при решении задачи является умение правильно отобрать и даже создать признаки. В англоязычной литературе это называется Feature Selection и Feature Engineering. Авторами использованы параметры, полученные исходя из длины и энтропии доменного имени, модели n-gram, а также модели TF-IDF(term-frequency, inverse document frequency). Классификация проводилась по принципу 80/20, т.е. обучение проводилось на 80% исходных данных, а тестирование алгоритма на оставшихся 20%. После тестировании качества классификации были получены следующие результаты:

Алгоритм	Legit/DGA	Многоклассовая
Logistic Regression	86,7%	78,8%
Random Forest	95%	89,3%
Naive Bayes	75,2%	75,6%
Extra Tree Forest	94,6%	88,9%
Voting Clasification	94,7%	89,9%

Как видно из результатов, была проведена классификация не только на вредоносные и легитимные домены, но и по принадлежности к определенному типу DGA. В многоклассовой классификации наилучший результат показал алгоритм Voting Classification. Данный алгоритм представляет собой классификатор выбора на основе результатов других статистических оценок. В выявлении вредоносных доменов лучше всего себя показал Random Forest.

Авторами предложен и апробирован улучшенный метод распознавания и классификации вредоносных доменных имен. Результаты качества классификации показывают, что эффективным алгоритмом выявления вредоносных доменов является Random Forest. Однако, его недостатком является высокий процент False-Positive, что существенно снижает практическое применение данного подхода. Также постоянное совершенствование алгоритмов генерации вредоносных доменных имен ведет к ухудшению качества данной модели. Таким образом, результаты работы показывают необходимость улучшения существующих подходов по обнаружению современных алгоритмов генерации вредоносных доменных имен.

Белов Н. И., Дубинич Е. А., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ В ЦЕЛЯХ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕНСОРНЫХ СЕТЯХ

Повсеместное распространение беспроводных самоорганизующихся сенсорных сетей приводит к необходимости обеспечения безопасности и стабильного состояния данных сетей.

Можно выделить следующие уязвимости БСС:

– Уязвимость каналов к прослушиванию и подмене сообщений, в связи с общей доступностью среды передачи, как и в любых беспроводных сетях.

– Незащищённость узлов от злоумышленника, который легко может получить один узел в распоряжение, так как обычно они не находятся в безопасных местах, таких как сейфы.

– Отсутствие инфраструктуры делает классические системы безопасности, такие как центры сертификации и центральные серверы, неприменимыми.

– Динамически изменяющаяся топология требует использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов или в результате изменения топологии.

– Бутылочное горлышко», когда две большие группы связаны одним устройством.

– Ограниченное (4–14) число каналов в диапазоне WiFi – приводит к засорению эфира.

– Проблема «темных углов» сети: наличие глухих мест, не связанных с другими ни через узлы одноранговой сети, ни посредством шлюзов.

Проявление некоторых данных уязвимостей можно описать как аномальное поведение устройств сенсорной сети. Обнаружение таких аномалий в сетях позволяет определять факторы/совокупность факторов, влияющих на сенсор, и определить степень опасности угрозы для сети в целом.

Мы предлагаем новый метод обнаружения аномалий в сенсорной сети, основанный на использовании коллаборативной фильтрации – особом методе оценивания и предсказания (в нашем случае) поведения устройств сенсорной сети. Преимуществами данного метода являются:

– высокая скорость реакции на любое воздействие;
– высокая степень информативности;
– качественная оценка причин отказа или пониженной работоспособности датчиков;
– повышение эффективности отслеживания уязвимостей в сети;
– возможность предсказания поведения устройств;
– обновляющиеся статистические данные;
– возможность предугадать сценарий атаки на систему или определенный участок сети, основываясь на прошлом опыте.

Исходя из этого, мы считаем данный метод обнаружения аномалий в сенсорных сетях актуальным и имеющим право на развитие и планируем реализовать его в программном эмуляторе и для анализа реальной сети.

Белов С. В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОПРЕДЕЛЕНИЕ ЭМОЦИОНАЛЬНОГО ОКРАСА ОБЩЕНИЯ ПОЛЬЗОВАТЕЛЯ С СОБЕСЕДНИКАМИ В МЕССЕНДЖЕРАХ

Автоматическая классификация текстов берет свое начало еще в 1960-х годах. Вплоть до 1980-х годов использовались методы, основанные на составлении правил, при помощи которых происходил анализ.

В настоящее время встает задача определения конкретного эмоционального оттенка (агрессивный, радостный, влюбленный и т. п.) сообщений собеседников в мессенджерах, как при использовании DLP-систем (анализ потока сообщений), так и в криминалистике при расследовании преступлений (анализ имеющейся переписки).

Целью является разработка системы, определяющей конкретный эмоциональный окрас подаваемого на вход сообщения или блока сообщений, переписки.

Задачами являются:

1. изучение существующих решений для русского и английского языков, анализ их применимости для поставленной цели;
2. построение математической модели системы;
3. создание программного комплекса.

Модель SentiStrength. SentiStrength оценивает величину положительной и отрицательной составляющих тональности в коротких, даже неформальных, текстах.

Отличительной особенностью данной модели является то, что она была создана для работы с короткими неформальными текстами с сокращениями и сленгом, то есть отлично подходит для анализа сообщений в мессенджерах или в Твиттере. Алгоритм оценивает каждый текст, подаваемый на вход, по двум шкалам одновременно: степень наличия негативной и положительной составляющих в тексте.

При проведении эксперимента были изучены пять эмоциональных окрасов: гневный, неприязненный, приязненный, радостный и нейтральный. После оценки сообщений программой полученные у каждого сообщения баллы по негативной и положительной шкалам были просуммированы. Таким образом, мы получили множество возможных значений Value1 = {−4, …, 4}.

Исследуемым окрасам были присвоены следующие значения: гневный = {−4, −3}; неприязненный = {−2, −1}; нейтральный = {0}; приязненный = {1, 2}; радостный = {3, 4}. В 26 случаях из 50 совпадают округленные числовые оценки экспертов и модели, в 27 случаях из 50 – текстовые значения (гневный, неприязненный и т. д.).

Модель Стэнфордского университета. Данная программа уникальна тем, что способна анализировать предложения, состоящие из одних и тех же слов, но размещенных в разном порядке, и при этом замечать изменившуюся тональность. Так, сочетания «странный, но приятный» и «приятный, но странный», имеющие разные эмоциональные окрасы, будут распознаны программой по-разному: в первом случае положительно, во втором – отрицательно. Модель оценивает тексты одной из пяти оценок: −−, −, 0, +, ++. Им были присвоены следующие эмоциональные значения: гневный = {−−}; неприязненный = {−}; нейтральный = {0}; приязненный = {+}; радостный = {++}. Также им были присвоены следующие числовые значения (для упрощения математического анализа): {−−} = −2, {−} = −1, {0} = 0, {+} = 1, {++} = 2. Таким образом, мы получили множество возможных значений Value2 = {−2, −1, 0, 1, 2}. В данной модели машинные оценки были намного хуже экспертных.

Для модели SentiStrength в целом результаты являются удовлетворительными, поскольку более чем в половине случаев результаты машинного анализа совпали с экспертными оценками. Способы улучшения результатов понятны и очевидны. Одним из базовых является внимательная работа со словарями, их расширение и более аккуратная разметка. При увеличении объема словарей программа сможет намного более точно оценить эмоциональную окраску как конкретного сообщения, так и всей переписки в целом.

Для модели Стэнфордского университета итоговые показатели оказались намного хуже, чем для первого алгоритма. Частично это объясняется небольшим размером экспериментальной выборки. Для улучшения показателей можно проанализировать исходный код программы, скорректировав его для собственных нужд.

В целом, задача определения конкретных эмоциональных оттенков (помимо «положительный»/«нейтральный»/«негативный») является очень сложной. Для более точного анализа нами предлагается использовать в моделях (в том числе и во вновь создаваемых) словари со словами-маркерами, характерными для определенных эмоций. Я считаю, что, используя словари подобного рода, удастся повысить частоту верного определения тональности общения. Так же важно анализировать контекст предложений, в котором размещаются слова из данных словарей, поскольку тональность сообщения может меняться в зависимости от того, как расположены слова, возможно использование сарказма, иронии и прочих языковых оборотов.

Бессонова Е.Е., Демяшев А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СОЗДАНИЕ РЕКОМЕНДАЦИЙ К АВТОМАТИЗИРОВАННЫМ СИСТЕМАМ УПРАВЛЕНИЯ (АСУ) «УМНЫХ ДОМОВ» (УД)

В настоящее время рынок решений по управлению “умными” домами и квартирами полон предложениями по контролю и оптимизации работы систем УД посредством единой автоматизированной панели управления. При разработке АСУ удобству полного управления всей системы УД придают больше значения, чем обеспечению безопасной работы пользователя. Нередко встречаются решения от разных производителей, находящиеся в открытом доступе, которые не имеют должной защиты от наиболее распространенных атак: перехват и подмена трафика от клиента к серверу; эксплуатация характерных конкретному производителю программного или технического обеспечения уязвимостей; и многие другие.

Многоуровневая и многофункциональная система управления УД обусловила необходимость разработки решений для системного тотального контроля за состоянием и функционированием как самой системы, так и за действиями пользователя.

Целью данной работы является выявление уязвимостей в АСУ, которые могут вывести УД из строя или нанести вред жизни и здоровью человека, и последующее составление рекомендаций для разработчиков АСУ по их недопущению на этапе разработки УД или же перекрытию на этапе эксплуатации.

Перекрытие технических каналов утечки информации, разграничение прав доступа к разным логическим уровням системы УД, контроль целостности и доступности элементов системы является неотъемлемой частью защиты для трех типов АСУ: локальная панель АСУ, мобильное приложение с доступом к АСУ, а также удаленный доступ к АСУ через сеть интернет.

В работе будут подробно рассмотрены каждый тип АСУ на наличие уязвимостей, выявлены недостатки систем УД в общем. На основе полученных результатов будет составлен перечень рекомендаций для АСУ по безопасному проектированию, разработке, внедрению в эксплуатацию и непосредственной эксплуатации систем “Умный Дом”.

Бессонова Е.Е., Настека А.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ПРОТОКОЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ ДЛЯ РЕАЛИЗАЦИИ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ПРИМЕРЕ СИСТЕМЫ «УМНЫЙ ДОМ»

Развитие систем домашней автоматизации породило проблему стандартизации протоколов передачи информации между управляемыми устройствами, датчиками и другими элементами «умного дома». Особенно остро стоит проблема, когда необходимо обеспечить конфиденциальность и целостность циркулирующих данных в АСУЗ.

Целью исследования является поиск защищенного сетевого протокола, позволяющего при его использовании в системе исключить влияние на конфиденциальность, целостность информации без использования специальных программно-аппаратных решений. Также необходимо обеспечить доступность устройств автоматизации путем отсутствия центральных управляющих блоков и возможности вести автономную работу.

Основные защищенные протоколы можно условно разделить на два больших класса: применимые при проводных решениях домашней автоматизации (например, IPsec, SSL, TLS); применимые при создании беспроводной системы (ZigBee, Z-Wave, Thread, WeMo). «Умный дом» имеет свои особенности реализации и, как правило, является надстройкой к уже существующей инфраструктуре, поэтому основным направлением анализа являются беспроводные протоколы, позволяющие удобно реализовать сетевое взаимодействие. Проводные решения стоит рассматривать только в условиях внедрения домашней автоматизации на ранних этапах строительства отдельных помещений или квартир, а также при проектировании критических элементов системы.

При использовании беспроводных протоколов и устройств появляется вопрос их возможности обеспечить надлежащий уровень конфиденциальности и целостности данных. Это связано влиянием на уже существующие беспроводные сети в зоне применения, распространенность протокола связи, возможность перехвата управляющего сигнала с его последующим анализом или атакой. Также имеются дополнительные требования по обеспечению доступности данных в «умном доме» и способности вести автономную работу.

В работе были рассмотрены 4 основных беспроводных технологии (ZigBee, Z-Wave, WeMo, Thread), с помощью которых можно реализовать систему автоматизации в защищенном исполнении. Они были проанализированы по следующим критериям:

- шифрование данных – возможность обеспечить конфиденциальность информации;
- применяемая топология сети – возможность создания децентрализованной инфраструктуры;
- обеспечение дополнительной доступности данных и автономности работы;
- скорость передачи данных.

Отдельно необходимо отметить вопрос о замене защищенных беспроводных протоколов на российские аналоги. Несмотря на то, что имеются особые протоколы передачи информации, используемые в АСУ ТП (например, ОВЕН) или беспроводная технология MeshLogic, технические особенности не позволяют их правильно применять в системах домашней автоматизации в текущем виде.

В результате анализа сделан вывод, что наиболее подходящей технологией является применение ZigBee. Она максимально позволяет закрыть проблемы обеспечения конфиденциальности, целостности и доступности данных в системах домашней автоматизации. Также интересен в ближайшем будущем протокол thread, который использует наиболее современные возможности, однако малый срок практического применения в мире и отсутствие дополнительной информации о применяемых устройствах не позволяет говорить о нем, как о полноценной замене ZigBee. Дальнейшей целью автора является проведение эксперимента по практическому анализу эффективности уровня конфиденциальности, целостности и доступности данных данным протоколом в сравнении с другими представленными в материале технологиями.

Викснин И.И., Юрьева Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИМИТАЦИОННАЯ МОДЕЛЬ ДЛЯ ОПТИМИЗАЦИИ ПОКАЗАТЕЛЯ ДОСТУПНОСТИ ИНФОРМАЦИИ В МОБИЛЬНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

С увеличением роли и места мультиагентных робототехнических систем (МРТС) в современном мире растет актуальность задачи обеспечения информационной безопасности (ИБ), трактуемой в узком смысле как обеспечение конфиденциальности, целостности и доступность информации в группировке. В контексте функционирования МРТС именно обеспечение доступности информации является одним из необходимых условий выполнения основной задачи группировкой автономных агентов.

Рассматривая группировку МРТС только с точки зрения обмена информацией, можно свести её к модели равнозначных агентов, что обеспечивает приведение задачи обеспечения доступности информации агентов МРТС к задаче «справедливого обмена» в децентрализованных одноранговых самоорганизующихся сетях типа peer-to-peer (P2P). Аналогом агентов-злоумышленников в сетях P2P является узлы-фрилоадеры, пытающиеся получить максимум информации, не отдавая ничего взамен. Обеспечение максимального доступа к информации рациональных узлов и снижение объема получаемых данных узлами-фрилоадерами позволит увеличить доступность информации в рамках системы.

Для решения этой задачи был разработан подход локального ранжирования: значение показателя «ранг» базируется на сведениях о получаемых и отдаваемых ресурсах; локальное ранжирование подразумевает расчет рангов узлом для ближайшего окружения; расчет глобальных рангов для всей сети невозможен, как в силу чрезмерной ресурсоемкости, так и в силу невозможности проверки аутентичности данных.

Модифицированный алгоритм, направленный на повышение доступности информации в группировке, предполагает «разумное жертвование» интересами узла в пользу задач группировки путем введения трансферных процедур. Трансферные данные – данные, которые один узел сети получает у другого для немедленной передачи запрашивающему узлу. Они не хранятся на узлах-посредниках, т.к. те могут быть в них не заинтересованы, а выступают простым передатчиком. Подобный подход позволит значительно увеличить ранг узла с точки зрения соседних.

В силу сложности аналитического описания процессов в группировке большой размерности проверка этого подхода подразумевает проведение модельных экспериментов. Для проведения эксперимента была модифицирована компьютерная модель, имитирующая работу P2P-сети. При помощи этой модели возможно проведение эксперимента, позволяющего выбрать критерий построения рангов, при котором заданные показатели достигнут лучшего результата в конкретных условиях функционирования МРТС.

Григорьева Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МЕТОД АНАЛИЗА ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАНАЛОВ БЕСПРОВОДНЫХ СЕТЕЙ

В последнее время беспроводные сенсорные сети получили массовое развитие и прочно вошли в повседневную жизнь. Они могут связать воедино глобальные компьютерные сети и физический мир. Объединенные в беспроводную сенсорную сеть, датчики образуют распределенную, самоорганизующуюся систему сбора, обработки и передачи информации.

Развертывание самоорганизующихся беспроводных сетей влечет за собой ряд вопросов, направленных на обеспечение безопасности итоговой инфраструктуры. К основным уязвимостям можно отнести возможность прослушивания каналов, посылку внешних пакетов, осуществление физического доступа злоумышленника к узлу, атаку «человек посередине», атаку перебора ключей и другие. Недостаточная мощность вычислительных ресурсов и компонентов самоорганизующихся беспроводных сетей, распределенность на большой площади и, очень часто, в недоступных местах, приводит к тому, что ключи распространяются с помощью широковещательных пакетов. Применяемые протоколы шифрования, WEP и WPA, имеют слабые алгоритмы и подвержены частому вскрытию, что не позволяет в полной мере обеспечить требуемый уровень защиты.

Таким образом, возникает необходимость разработки моделей и методов анализа информационной безопасности беспроводных сетей.

Предложен подход к обнаружению аномально функционирующих устройств в самоорганизующихся беспроводных сетях на базе анализа статистических закономерностей откликов от удаленных устройств.

Определены направления повышения показателя доступности удаленных устройств беспроводных сетей, основанные на объеме пересылаемых пакетов для различных режимов работы.

Гусев Р.А.
Россия,Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИВАТНОСТЬ В ИНТЕРНЕТЕ

С каждым годом количество интернет-пользователей становится больше, только в России число таковых составляет 78.2 млн. или 68% населения, а так же и объем предоставления пользовательских данных в сети, ведь сегодня онлайн можно сделать практически все: от оплаты коммунальных услуг до покупки авиабилетов. К сожалению, с этим одновременно растет и количество киберпреступлений, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием интернета, являетсямошенничество.

В данный момент существует как минимум 10 вариантов кражи злоумышленником чужие логины и пароли, но от них можно защититься. Рассмотрим эти способы.

Различные интернет сервисы хранят большой объём персональных данных, такие как местоположение, подробные сведения об использовании служб, включая поисковые запросы, сведения об устройствах, такие как модель, версия операционной системы, номер телефона, реквизиты кредитной карты и многие другие. Рассмотрим, как и где они хранятся и в каких случаях их используют.

Ефремов А.А., Бессонова Е.Е., Канев А.Н., Никифорова К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

МОДЕЛИРОВАНИЕ СИСТЕМЫ, ПОСТРОЕННОЙ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ» КАК ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ

Умныйдом–автоматическаясистемауправлениязданием.
Под«умнымдомом»следуетпониматьсистему,
котораяпомогаетчеловекуобеспечитьполныйконтрольимониторингвсехинженерныхсистемздания.
Например, функциямисистемыявляютсяуправлениеэлектроникойиэлектрикойвдоме, защитаотчрезвычайныхпроисшествий: пожаров, протечекводы, газаит.д. Но, ксожалению, однимизсерьезныхнедостатковсистем«Умногодома»являетсянизкийуровеньзащищенности, чтоподтверждаетсямногочисленнымиисследованиями. Также, внастоящеевремяпрогнозируетсяростчислаправонарушений,
связанныхсумнойтехникойвцеломиумнымидомамивчастности.

Цельюданнойработыявляетсявыявлениеуязвимыхместсистем,
построенныхпотехнологии«Умныйдом».
Выявлениеуязвимыхместбудетпроизводитьсянаосновемоделисистемы.
Длядостиженияданнойцелибылипоставленыследующиезадачи:

- декомпозициясистемы«Умныйдом»;
- определениевзаимосвязеймеждукомпонентамисистемы;
- выбориобоснованиеметодамоделированиясистемы;
- разработкамоделисистемы;
- выявлениеуязвимостейсистемынаосновемодели;
- разработкарекомендацийпоустранениюуязвимостей.

Планируетсяразработатьмодель,
отображающуюустройствосистемыивзаимодействиееэлементовмеждусобой.
Припомощиданноймоделивдальнейшембудутпроводитьсяэкспериментыпоопределениюнадежностиси стемы, атакжебудутсимулироватьсяразличныеатаки.

Зайцева Н.М.
Россия, Санкт-Петербург, Санкт-петербургский национальный исследовательский университет информационных технологий, механики и оптики

ПРИМЕНЕНИЕ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ ДЛЯ ПЛАНИРОВАНИЯ ЗАТРАТ НА СИСТЕМУ БЕЗОПАСНОСТИ

В современном мире владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде деятельности. Информация используется для принятия важных стратегических решений, и от ее полноты достоверности и актуальности зависит дальнейшее развитие компании. Именно поэтому задача обеспечения безопасности информационных ресурсов становится все более значимой.

Часто для обоснования и расчета инвестиций в систему безопасности используется анализ информационных рисков, который связывает возможные угрозы со значимостью ресурсов системы.

Наиболее известные методы оценки: качественный и количественный анализ.

Суть качественного анализа рисков заключается в оценке значений риска экспертами. Данный метод используется, когда сам риск не может быть измерен количественно и описан математически.

Количественный анализ предполагает численное определение величин отдельных рисков и риска проекта в целом. Количественная оценка применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени, человеческих ресурсах и т.д

На практике распространен упрощенный подход к обоснованию системы обеспечения безопасности, который не требует расчета рисков для конкретного объекта. Данный метод представляет собой проверку соответствия уровня защищенности объекта требованиям одного из стандартов в области информационной безопасности.

Сравнив существующие подходы к оценке рисков, можно сделать вывод, что только количественная оценка дает требуемый результат - позволяет конкретно рассчитать и аргументировать затраты на создание системы защиты.

В ходе подробного изучения метода были выявлены проблемы, которые необходимо рассматривать более детально и находить пути их преодоления.

Существует подход, способный облегчить количественный анализ рисков. Он основан на принципе «разумной достаточности», примененном к сфере обеспечения информационной безопасности.

Оценка риска подразумевает оценку стоимости ущерба, частоты возникновения негативных событий и вероятности того, что событие повредит ресурсу.

Размер ущерба от реализации угрозы для конкретного ресурса зависит от стоимости ресурса, подверженного риску, и от степени разрушительного воздействия на ресурс.

Степень разрушительности можно выразить коэффициентом разрушительности, возможные значения которого лежат в диапазоне от 0 до 1.

Оценив за конкретный период частоту возникновения негативного события (например, за год) и вероятность реализации угрозы, получаем формулу стоимости риска.

Количественный анализ информационных рисков представляет собой достаточно объемную и трудоемкую задачу, но его целесообразность и эффективность не вызывает сомнений. Он позволяет определить необходимую сумму инвестиций в безопасность и обеспечить должный уровень понимания проблемы обеспечения информационной безопасности со стороны руководства.

Золотарева Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СИСТЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ КАК СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

В последнее время отмечается рост интереса организаций к автоматизации управления привилегированных учетных записей, которые используются как внутренними привилегированными пользователями, так и внешними привилегированными пользователями.

Бесконтрольное использование таких учётных записей, в частности, отсутствие регулярной смены паролей и контроля действий администраторов может привести к инцидентам, связанным со сбоями ОС, средств виртуализации и оборудования, вызванными ошибочными или злонамеренными действиями привилегированных пользователей.

Ввиду этого наиболее активное развитие на современном этапе получают решения, связанные с защитой баз данных, поскольку именно они являются одним из наименее охваченных направлений в области защиты конфиденциальной информации. В качестве примера можно рассмотреть компанию, имеющую собственную базу данных SQL, в которой содержится конфиденциальная информация. Пользователь, обладающий привилегированными правами доступа, может получить выгрузку этих данных, используя вполне легальные средства и легальные инструменты, которые компания сама предоставила ему для работы. После выгрузки информации из базы отслеживать ее распространение становится сложно. Ввиду этого разрабатываются определенные системы, которые позволяют анализировать запросы, обращенные к базам данных, и, исходя из этого, определять – какую информацию из базы данных пользователь намерен получить. Подобная работа системы обеспечивает защищенность на уровне сетей и представляет собой отдельный класс продуктов, никак не связанный с DLP-системами. Такого рода системы позволяют защитить как саму базу данных, так и информацию, хранящуюся в ней – системы контроля привилегированных пользователей.

На сегодняшний день очень сложно контролировать привилегированных пользователей без применения специализированных средств и среди систем широкое распространение получили системы контроля привилегированных пользователей в частности аналитические или дополнительные системы, контролирующие права доступа к целевым бизнес-ресурсам.

Аналитические системы контроля привилегированных пользователей призваны решить проблемы сбора и анализа информации, представления ее в удобном для пользователей виде.

Данные системы предназначены для решения широкого спектра аналитических задач. Для решения специализированных задач, в частности для автоматизации процессов планирования, анализа и контроля показателей эффективности деятельности предприятия используются системы управления эффективностью бизнеса (CorporatePerformanceManagement, CPM).

Золотарева К.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ОРГАНИЗАЦИОННЫХ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ЛАЗЕРНЫМ МИКРОФОНАМ

Организационная защита информации — это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение информацией ограниченного доступа и проявление внутренних и внешних угроз.

Поэтому необходимо проводить мероприятия по организационной защите, учитывая возможности и условия эксплуатации лазерных микрофонов, основываясь на принципе их работы и возможных технических характеристиках. Не стоит недооценивать злоумышленника.

К применению организационных мероприятий необходимо подходить разумно. Следует уделять особое внимание помещениям, в которых проводятся важные совещания, переговоры, конференции.

Также нельзя забывать и про режимные средства, которые обеспечивают порядок допуска и доступа людей в то или иное помещение.

Неплохой способ контроля — установить внутри помещения скрытую камеру с круглосуточной записью. Это даст возможность фиксировать все действия персонала, а при необходимости восстановить события.

Если же важность информации невелика, то следует ограничиться только некоторыми мероприятиями.

Неплохие результаты дает и зашумление помещения, в котором идут переговоры. Зашумление рекомендуется производить специализированной аппаратурой (от 500 долл.), но можно воспользоваться и просто заранее подготовленной записью шума. В качестве зашумления можно использовать и звуковой фон помещения с большим количеством людей.

Значительные трудности для злоумышленника создаст непредсказуемость действий объекта наблюдения.

Организационные мероприятия играют существенную роль в методах противодействия лазерным системам. Влияния организационных аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность негласного съема конфиденциальной информации.

Немаловажным является оценка размера затрат на защиту от лазерных микрофонов. Как отмечалось ранее, лазерные системы имеют очень высокую стоимость.

Вопросы оценки эффективности затрат в области информационной безопасности всегда актуальны и требуют грамотного решения. Лазерный микрофон при грамотной эксплуатации – эффективное средство негласного съема информации. Безусловно, полный комплекс применяемых средств и способов защиты стоит дорого. Прежде чем принимать решение об организации защиты данного канала утечки информации, стоит задуматься над тем, а «надо ли это». Если действительно есть что скрывать, и стоимость информации значительна, то стоит выделить средства для обеспечения полноценного комплекса защиты сведений ограниченного доступа.

Нецелесообразно в случае, если ценность информации невелика, применять дорогостоящие средства защиты и осуществлять все организационные мероприятия. Техника защиты информации достаточно дорогая, но если возможные убытки от перехвата информации выше — на защите экономить не стоит. Службы безопасности должны уметь разумно оценить необходимость защиты информации от лазерного микрофона. Правило, которым следует руководствоваться при организации защиты: затраты на защиту информации не должны превышать цену защищаемой информации.

Организация защиты информации от перехвата информации лазерными микрофонами возможна различными способами и средствами. Необходимо проведение оптимизации всех применяемых мер защиты при их комплексном использовании, тем самым обеспечивая защиту на разных уровнях. Наличие большого количества противоречивых требований и ограничений требует проведения многоспектральной оценки эффективности системы защиты объекта от лазерных систем перехвата речевой информации, так как при несогласованности между собой отдельных аспектов безопасности риск «проколов» в технологии защиты увеличивается.

Стоит отметить, что сейчас отсутствуют дешевые автоматические средства обнаружения использования лазерного микрофона, и возможным направлением дальнейшего рассмотрения вопроса защиты речевой информации от негласного съема с помощью лазерного микрофона может являться применение подобных систем. Значительным преимуществом таких систем будет возможность автоматического определения местоположения источника излучения, что в свою очередь облегчит задачу обнаружения факта ведения наблюдения.

Игнатьев М.Б.,Бариков Л.Н., Литовкин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРОБЛЕМА БОРЬБЫ С АСТЕРОИДНОЙ ОПАСНОСТЬЮ И КОСМИЧЕСКИМ МУСОРОМ

Астероидная опасность угрожает всему человечеству, а космический мусор – искусственным спутникам и пилотируемым кораблям. Существует множество проектов борьбы с астероидами, которые направляются к нашей планете. В докладе анализируется и моделируется система «Гравитационный тягач» для того, чтобы вовремя отклонить летящий астероид от столкновения с Землей. Гравитационный тягач – это спутник весом около 10 тонн, который должен быть размещен рядом с астероидом таким образом, чтобы изменить его траекторию. При этом возникают сложные задачи обеспечения надежной работы системы в открытом космосе на протяжении нескольких лет. Рассматривается проблема борьбы с космическим мусором на основе создания специальных спутников – пожирателей мусора.

Иванова Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,

ВЫБОР ПАРАМЕТРОВ КЛАСТЕРИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБНАРУЖЕНИЯ АТАК

Статистика возникновения атак показывает, что злоумышленные действия над информацией не только не прекращаются, а имеют достаточно устойчивую тенденцию к росту. Атаки на информационные системы становятся всё разнообразнее и для обнаружения и предотвращения некоторых из них необходимы новые средства защиты. А потому актуальным является любое повышение эффективности обнаружения атак.

Реализация атак, направленных на отдельные компьютеры, приводит к возникновению событий в операционной системе. Анализируя эти события, можно увидеть какие-либо отклонения в работе системы, что позволит сделать вывод о совершении атаки на систему.

В Windows слежение за состоянием системы можно осуществлять с помощью журналов событий, мониторинга производительности, а также информации о процессах, запущенных в текущий момент времени. Сведения о событиях, связанных с наиболее критичными объектами операционной системы регистрируются и сохраняются в журналах Windows.

С точки зрения обнаружения атак наиболее информативными являются события, отраженные в журналах безопасности.

В связи с тем, что число новых, ранее неизвестных атак растет с каждым годом, наиболее предпочтительными к использованию являются адаптивные методы обнаружения вторжений, т.к. они позволяют обнаруживать атаки, отличные от ранее известных.

Для исследования выбран метод кластерного анализа. В результате анализа наиболее распространённых алгоритмов кластерного анализа в качестве наилучшего был выбран алгоритм k-средних, так как он довольно прост для реализации и запуска, относительно быстрый, легко адаптируется и распространен на практике.

Пространство событий, происходящих в операционной системе, является многомерным пространством, сложным для описания. В процессе кластеризации оно разбивается на подпространства. Необходимо экспериментально определить наилучшее с точки зрения количества ошибок кластеризации количество подпространств, на которые выполняется разбиение. Оно соответствует количеству используемых в процессе кластеризации кластеров k.

Другими характеристиками выбранного метода кластеризации, влияющими как на точность отнесения событий к заданным кластерам, так и на скорость обучения и функционирования метода, являются мера близости, применяемая при кластеризации, и способ первоначального выбора центров кластеров.

Таким образом, объектом исследования является метод кластерного анализа, предметом – влияние используемых параметров кластеризации на эффективность обнаружения атак, а дальнейшее исследование направлено на проведение экспериментальных исследований путем имитационного моделирования и подбор наилучшей комбинации выделенных параметров метода. Критерием качества полученного результата является количество ошибок, время обучения и время реакции на новое событие.

Каждое событие обладает определенным набором полей уровень, дата и время, источник, код события, категория задачи, пользователь и т.д. Но не все поля журнала имеют одинаковую информативность. Поэтому наибольший интерес для анализа представляют следующие поля: уровень, дата и время, код события. Именно по ним и осуществляется разбиение событий на кластеры.

В результате проведения сорока экспериментов с варьированием значений изменяемых параметров метода k-средних для каждого эксперимента получены значения: ошибок 1-го рода, ошибок 2-го рода, времени обучения и времени реакции на новое событие.

Для анализа результатов экспериментальных исследований рассчитано значение показателя, оценивающего качество набора входных параметров.

Таким образом, наилучшей комбинацией параметров является: количество кластеров – 4; способ начального выбора центроидов - случайный выбор k наблюдений; используемая метрика – расстояние Чебышева.

Полученные результаты могут быть использованы для повышения эффективности обнаружения атак.

Ильин А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

РАЗРАБОТКА СИСТЕМЫ ПРОГРАММНО-АППАРАТНОГО ШИФРОВАНИЯ КАНАЛА СВЯЗИ НА БАЗЕ МИКРОКОНТРОЛЛЕРОВ ФМК

В условиях постоянного развития и расширения сетей средств вычислительной техники вопрос обеспечения защищенности связи между различными устройствами приобретает все большую актуальность. В данном докладе рассматривается создание аппаратного блока, позволяющего защищать информацию, передаваемую по проводному каналу связи посредством применения алгоритма симметричного блочного шифрования.

Существует два основных способа шифрования информации, передаваемой по каналам связи: программный и аппаратный(аппаратно-программный). Программный способ предполагает наличие на принимающей и передающей стороне специализированного программного обеспечения, выполняющего функции шифрования и дешифрования передаваемых и поступающих сообщений. Данный способ, несмотря на простоту установки защиты, имеет ряд недостатков. Во-первых, программное обеспечение имеет множество требований, сужающих спектр устройств, на которые оно может быть установлено. Во-вторых, функционирование программы зависит от ОС устройства, что уменьшает отказоустойчивость, а также создает угрозу безопасности передачи информации, поскольку предполагаемый злоумышленник может организовать атаку на устройство и получить доступ к ключам шифрования и сам алгоритм, что сведет эффективность защиты передаваемых данных к нулю.

Применение аппаратного(аппаратно-программного) способа шифрования данных лишено многих недостатков, присущих первому способу. Устройство шифрования в данном случае представляет собой подключаемый к средству вычислительной техники блок либо встраиваемую в него плату расширения, работа которых не зависит от параметров СВТ, к которому он подключен. Таким образом, устройство может представлять собой «черный ящик», доступ к которому можно как угодно затруднить как с физической, так и с иных сторон. Подобное решение для шифрования данных защищено от взлома путем воздействия на устройство, передающее информацию для шифрования в силу того, что между ними происходит только обмен данными, подлежащими приему и передаче. Недостатком данного способа является дороговизна шифровальной системы.

Разрабатываемая система шифрования канала связи предполагает создание блока шифрования/дешифрования на базе микроконтроллера Atmel выбранного в силу распространенности, относительной дешевизны, а также наличия их отечественных аналогов, разработки максимально простого протокола создания и передачи пакетом, несущих как можно большее количество значимой информации. В качестве рабочего материала используется микроконтроллер Atmega128. Предполагается, что прототип, полученный после завершения разработки, будет представлять собой блок шифрования/дешифрования, подключаемый к СВТ через COM-порт либо USB –интерфейс и передающий/принимающий данные по стандарту RS-485. Так как часть устройства, отвечающая за шифрование и дешифрование данных, не будет зависеть от интерфейса передачи и получения данных и физической природы канала связи, появится возможность его изменения под появляющиеся нужды.

Ильин И.В., Бессонова Е.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

«УМНЫЙ ДОМ» КАК МУЛЬТИАГЕНТНАЯ СИСТЕМА ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Технологии умного дома в настоящий момент очень активно набирают популярность. Составной частью системы «Умный дом» являются различного рода сигнализации и датчики (движения, задымления, датчики открытых дверей и окон, системы видеонаблюдения), которые помогают обеспечить безопасность квартир, коттеджей и других жилых помещений, в которых установлены данные системы. Также существует возможность внедрения специального

встраиваемого оборудования, используемого правоохранительными органами и частными охранными предприятиями, которое позволяет отслеживать неразрешенную деятельность на контролируемой территории.

В системе «Умный дом» можно выделить несколько подсистем, например, таких как электроснабжение, водоснабжение, освещение, кондиционирование и вентилирование и прочие.При фиксировании датчиками одной подсистемы наличия чрезвычайной ситуации(пожар, возгорание, прорыв трубы, затопление, землетрясение и т.д.), данная подсистема должна отреагировать приемлемым образом и решить, необходимо ли привлекать другие подсистемы к ликвидации возникшей чрезвычайной ситуации. Также можно отметить, что проблема должна быть решена с минимальными последствиями для дома. Например, при фиксировании возгорания и присутствии хозяина дома, системе достаточно сообщить об источнике возгорания, чтобы тот потушил его самостоятельно, вместо проведения целого комплекса мероприятий предотвращения пожара, затрагивающего практически все подсистемы умного дома.

При рассмотрении системы «Умный дом» как мультиагентной, каждаяподсистема умного дома, по сути, будет являться агентом данной системы.В работе рассматривается и анализируется поведение и взаимодействиеподсистем умного дома как мультиагентной системы при чрезвычайных ситуациях.

Иоффе М.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЛАЗЕРНОГО МИКРОФОНА И РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕР ПРОТИВОДЕЙСТВИЯ

Опасность ЛСАР связана это с тем, что такие системы позволяют снимать речевую информацию с высоким качеством на больших расстояниях, без необходимости проникновения в помещение, а выявление съема в большинстве случаев невозможно. Таким образом, в связи с прогрессивным развитием и совершенствованием ЛСАР, задачи связанные с организацией защиты от таких ТСР очень актуальны.

Лазерные микрофоны позволяют воспроизводить речь при лазерно-локационном зондировании оконных стекол и других отражающих поверхностей.

В настоящее время изобретено и предложено к использованию множество решений по обходу стандартных средств защиты от ЛСАР и улучшению качества и удобства работы этих систем. В ближайшем будущем, судя по уже имеющимся разработкам, защищаться от таких микрофонов станет возможно, только применяя целый комплекс мероприятий по закрытию этого канала утечки информации.

В рамках работы была создана схема принятия решений, которая поможет грамотно оценить необходимость защиты от ЛМ. В ней учтены расположение ОЗ, инструментальные и расчетные методы определяющие дальность перехвата опасного сигнала, сравнение дальности с радиусом КЗ, и, в случае принятие решения о необходимости защиты – предпринимаемые действия.

Основное условие выбора мероприятий при защите от ЛМ является минимизация затрат, и выбора только необходимых для конкретного объекта защиты.

Существует несколько эффективных методов пассивной защиты, которые могут существенно снизить вероятность снятия информации лазерным микрофоном: нанесение на стекло неровных, шероховатых материалов, которые способствуют диффузному отражению лазерного луча; периодическое приоткрывание окон; наблюдение за обстановкой в соседних зданиях и на улице; проведение переговоров, не повышая голоса; все конфиденциальные переговоры переносятся в помещения без окон или в подвальные, полуподвальные помещения; использование погодных и климатических условий (дождь, снег); ведение переговоров в местах с высоким уровнем фоновых шумов (как внешних, так и внутренних) без учета активной защиты; размещение на местности таким образом, чтобы на пути распространения лазерного луча были естественные и искусственные препятствия (кустарник, строения и т. д.); увеличение расстояния от говорящего до окна.

Активные меры защиты заключаются в создании маскирующих акустических помех средствам разведки, то есть использование виброакустической маскировки информационных сигналов, которое снижает отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи).

Чтобы оценить достаточность уровня шума, генерируемого устройствами активной защиты, было использовано соотношение сигнал/шум лазерного микрофона, которое поступает на оконечное устройство.

Сравнивая результат с уровнем, пороговым для восприятия акустического сигнала, можно оценить возможность перехвата и, соответственно, степень информационной защищенности выделенного для конфиденциальных переговоров помещения.

Таким образом, было выявлено, что шум создаваемый устройством активной защиты должен превышать имеющийся минимум на 15 дБ.

Лазерные средства акустической разведки имеют ряд значительных недостатков и множество способов как пассивной, так и активной защиты. Поэтому, если организация защиты от лазерного микрофона проводится превентивно, с учетом всех основных рекомендаций с привлечением опытных специалистов, реализация приемлемой эффективной защиты от утечки по рассмотренному каналу может считаться достижимой.

Также можно сделать вывод, что в настоящее время, необходима разработка системы, позволяющей автоматизировать процесс обнаружения источника системы перехвата.

Канев А.Н., Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТРИК

Обеспечение информационной безопасности является неотъемлемой частью деятельности современного информационного общества. Важной проблемой в данном процессе является определение уязвимостей системы, в том числе информационных систем.

Анализ уязвимостей информационных систем включает в себя процедуры выявления и оценки уязвимостей. С целью выполнения первой процедуры разработаны инструментальные средства, такие как сканеры уязвимостей, при этом используются базы данных уязвимостей (например, Common Vulnerabilities and Exposures). Для выполнения второй – методики оценки уязвимостей (например, Common Vulnerability Scoring System), а также экспертные оценки. Недостатками существующих средств и методов является рассмотрение лишь уязвимостей программного обеспечения, отсутствие взаимосвязи процедур выявления и оценки уязвимостей, а также субъективный характер экспертных оценок.

Целью работы является разработка методики анализа уязвимостей, которая не обладает указанными недостатками.

Методика рассматривает уязвимости технических средств, программного обеспечения, линий связи, инфраструктурные и организационные уязвимости информационной системы и классифицирует данные уязвимости по классам. С целью анализа уязвимостей предлагается использовать инструментальные средства для сбора информации об уязвимостях отдельных классов и таким образом определять значения метрик классов уязвимостей. При формировании оценки уязвимостей предлагается использовать метод парных сравнений для расчета приоритетов метрик, которые необходимы для вычисления степени опасности уязвимостей класса. Полученные значения степени опасности применяются для определения степени опасности уязвимостей как отдельных компонентов информационной системы, так и информационной системы в целом.

На данный момент разработана модель оценки уязвимостей, выделены классы уязвимостей, формируется перечень метрик, используемых для оценки. Для реализации методики был разработан программный модуль на платформе RSA Archer.

Преимуществами данной методики является охват широкого спектра уязвимостей с использованием единого подхода к их оценке. Также разработанная методика позволяет добиться более объективного анализа за счет снижения роли эксперта в данном процессе. Результаты ее применения служат исходными данными для оценки рисков информационной системы.

В дальнейшем планируется улучшение сформированного перечня метрик, опытная эксплуатация разработанной методики и сравнительный анализ с аналогами.

Карбутов Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ВСЕ ЕЩЕ ЖИВОЙ NTLM

Информационные технологии уже давно проникли во все аспекты жизни человека – работа, бизнес, здоровье, дом и т.д. Все от самых мелких до самых крупных компаний используют компьютеры для автоматизации и упрощения работы. И самой популярной системой была, остается и будет в ближайшем обозримом будущем – это Windows. Windows имеет много различных вариаций как для домашнего использования, так и для создания и управления огромными локальными сетями, веб-серверами и т.д. Исходя из такой популярности данной системы тема информационной безопасности очень актуальна. Для поддержания уровня безопасности компании пользуются услугами компаний, которые проводят аудит.

Особенностью ОС Windows является протокол NTLM, который используется для большей части взаимодействий по сети среди машин оснащенных данной системой. Хотя протокол был разработан достаточно давно, его поддержка до сих пор продолжается, т.к. в нем находят все новые и новые уязвимости. В своей работе я проводил исследование протокола, чтобы определить новую уязвимость или возможность, которую можно использовать при аудите таких систем.

Во-первых, мной был исследован сам протокол NTLM. Во-вторых, приведены рекомендации по эксплуатации различных автоматизированных средств и техник по разным категориям (методы и средства взлома хешей, извлечение аутентификационных данных их хранилищ, атаки на системы с использованием протокола). В-третьих, мной было найдено слабое место в документах формата docx, которое позволяло украсть хеш пароля пользователя без какого-либо подтверждения, используя специально сформированный документ. В-четвертых, разработано автоматизированное средство на языке python, которое позволяет создавать специально сформированный документ, который использовал данную слабость системы.

Исходя из выше сказанного, мной была доказана актуальность данной технологии на деле. Несмотря на то, что данный протокол постоянно улучшается, в нем все равно существуют уязвимости, которые можно применять при аудите систем с использование ОС Windows.

Келесис Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СОЗДАНИЕ СПРАВОЧНОГО ПОСОБИЯ, ПОВЫШАЮЩЕГО УРОВЕНЬ ИБ, НА ОСНОВЕ ИССЛЕДОВАНИЯ ВЕКТОРОВ АТАК НА СУБД MSSQL SERVER

С каждым днем информационные технологии все быстрее проникают в повседневную жизнь человека. Компании, промышленные заводы, крупные предприятия используют информационные системы для автоматизации своих производственных процессов. Вся конфиденциальная информация, секреты производства, бухгалтерия, персональные данные, хранятся в системе управления базами данных. Обеспечение безопасности такого ключевого звена, как СУБД, является одной из самых важных задач специалиста по защите информации. С развитием информационных систем растут и атаки на них. Безопасное внедрение и администрирование СУБД в организацию является трудоёмким процессом и, как правило, имеют низкий уровень информационной защищенности. Злоумышленники, получившие доступ к СУБД могут нанести колоссальный вред бизнес-процессу, а также репутации предприятия.

Система управления базами данных (СУБД) – специализированный комплекс программ, использующийся для эффективной и удобной организации, мониторинга и администрирования баз данных. Их особенностью является наличие процедур для ввода и хранения не только данных, но и описания их структуры. Внедрение СУБД на предприятии становится неотъемлемой частью проектирования информационной системы, так как она предоставляет большой диапазон возможностей по хранению и обработке больших массивов данных.

СУРБД Microsoft SQL Server – комплексная платформа БД, позволяющая управлять данными в масштабе организаций. СУБД имеет встроенные, сертифицированные по требованиям безопасности, средства защиты информации, позволяющие обрабатывать персональные данные и конфиденциальную информацию.

Microsoft SQL Server является одной из самых распростарненных СУБД в мире, занимая третье место по версии DB-Engines. Исследование безопасности СУБД выявило, что она подвержена различным видам уязвимостям, таких как: перебор пользователей БД методом грубой силы, повышение привилегий через хранимые процедуры, обход локальной авторизации, копрометация через связи между базами данных. Данные векторы имеют разную степень критичности, при этом некоторые из них могут быть проэксплуатриованны только внутренними нарушителями, другие же как внутренними, так и внешними, что повышает риск для организации.

В процессе исследования векторов атак на СУБД MSSQL Server было выявлено, что большинство угроз, потенциально реализуемых злоумышленником, появляются на стадии конфигурирования БД и создания приложений, взаимодействующих с СУБД.

Для повышения уровня защищенности, были созданы справочные пособия, в которых описываются небезопасные значения параметров, конфигурационных файлов, и значения, рекомендуемые для безопасной работы СУБД.

Результаты данной работы могут быть использованы системными администраторами и разработчиками приложений, взаимодействующие с СУБД Microsoft SQL Server, для повышения безопасности своих продуктов.

Значимость работы для информационной безопасности заключается в акцентировании внимания на проблемы хранения и обработки массивов данных в СУБД MSSQL Server. В результате исследования было выявлено, что неправильная конфигурация отдельных компонентов может быть использована злоумышленников для компрометации информационной системы. Для обеспечения

комплексной безопасности, защита должна происходить так же на уровне приложений, взаимодействующих с СУБД. Предложенные методы позволят существенно сократить количество векторов атак и повысить безопасность СУБД.

Кудрявцева К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ВОЛОКОННО-ОПТИЧЕСКОГО КАНАЛА СВЯЗИ ОТ УГРОЗЫ ПЕРЕХВАТА ТРАФИКА

Роль информации в современном обществе повышается, и все большее внимание уделяется защите информации от различного вида угроз и атак, поскольку развитие информационной техники создает все новые и неизвестные каналы утечки информации. Особую опасность несут технологии, которые используют ранее не известные физические принципы реализации процессов.

Любое современное предприятие не может обойтись без использования глобальной сети Internet, для связи как между сотрудниками внутри организации, так и для взаимодействия с различными органами исполнительной власти. Информацию, которую передают или получают сотрудники, можно объединить в понятие «интернет-трафик».

Как раз эта информация может быть перехвачена, модифицирована или удалена при подключении к ВОЛС, что принесет предприятию убытки в денежном эквиваленте, часто не малые.

Таким образом, можно выделить одну из главных угроз безопасности информации, передаваемой по ВОЛС - угроза перехвата трафика.

Условно можно выделить три основные группы методов, предотвращающих или снижающих до минимума влияние посторонних подключений.

Первая группа - наблюдение за кабелем и мониторинг.

Этот способ заключается в использовании различных технических средств защиты информации от перехвата и включает большой набор активного оборудования, используемого при вводе в эксплуатацию смонтированных волоконно-оптических линий передачи информации.

В настоящее время разработана и широко используется измерительная аппаратура, позволяющая не только определять с высокой точностью величину полных потерь в линии (мультиметры), но и распределение потерь вдоль неё (оптические рефлектометры).

Мультиметр может использоваться как стабилизированный источник излучения, измеритель оптической мощности и затухания оптического сигнала в процессе прокладки, эксплуатации и ремонта волоконно-оптических линий связи. С применением этого прибора можно установить общие параметры работающей ВОЛС.

Так же используются оптические тестеры.

Аппаратные средства защиты — средства защиты информации, реализованных на аппаратном уровне. Этот метод представлен кодовым зашумлением.

Он заключается в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декодировании сигналов, получаемых из канала утечки информации.

И третий метод – шифрование, хотя оно никак не препятствует подсоединению к волокну, оно делает украденную информацию малополезной для злоумышленников.

В настоящее время, в сфере волоконно-оптических технологий широкое применение нашла квантовая криптография. Это обусловлено тем, что с ее помощью возможна передача фотонов света на большие расстояния и с малыми искажениями.

В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики - фотонов.

Необходимость в современной квантовой криптографии заключается в безопасном (конфиденциальном) распределении криптографических ключей между двумя абонентами без предварительного обмена секретами. Несмотря на схожесть решаемых задач с задачами традиционных асимметричных протоколов распределения ключей, принципы квантовой криптографии в корне отличаются от основ традиционной.

В заключении отметим, что каждый из этих методов по-отдельности не сможет полностью защитить информацию ограниченного доступа, от попадания ее за пределы контролируемой зоны, поэтому, чтобы минимизировать такую вероятность, нужно применять комплекс указанных мер, а так же проводить работу с персоналом.

Кузьмич Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

СТАНДАРТЫ СПЕЦИФИКАЦИИ МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

Методы разработки агентных систем имеют свои специфические особенности, в виду которых подходы, пригодные для, к примеру, разработки программного обеспечения, не применимы в отношении мультиагентных робототехнических систем.

В частности, существующие методики не могут учесть и соответственно фиксировать автономное, распределенное поведение агентов, множество путей взаимодействия между агентами, сложность организационной структуры и множество подходов к распределению и достижению целей. Поэтому были разработаны различные методики и стандарты, которые в настоящий момент применяются для проектирования и анализа мультиагентных робототехнических систем.

В частности известны несколько мультиагентных платформ, которые успешно используют абстрактную спецификацию FIPA-2000, созданную некоммерческой организацией FIPA (Foundation for Intelligent Physical Agents) с целью обеспечения совместимости различных мультиагентных систем, отвечающих данным стандартам. Архитектуру FIPA успешно применяют такие агентные системы как FIPA-OS компании Nortel Networks (Великобритания) или JADE компании CSELT (Италия).

В рамках данной архитектуры агенты общаются друг с другом при помощи обмена сообщениями, закодированными на языке ACL (agent communication language). FIPA определяет три основные службы: справочная служба агентов, справочная служба сервисов, а также служба транспорта сообщений, реализующая функцию обмена и коммуникации между агентами.

Организация OMG преследовала цель стандартизировать конкретные области спецификации агентных систем, а именно:

- технологии мобильных агентов;
- менеджмент агентов;
- трансфер агентов;
- именование агентов и агентных систем;
- типы агентных систем;
- синтаксис местоположения;

Архитектура FIPA разработана более подробно, чем OMG, и учитывает стандарты регистрации агентов, а также вопросы регистрации и использования сервисов, т.е. необходимого функционала в рамках агентной системы. С другой стороны, в отличие от спецификации MASIF, которая обеспечивает совместимость агентных систем, написанных на одном языке, но от разных производителей, ядром архитектуры FIPA являются вопросы коммуникации агентов, которые в MASIF и OMG фактически рассмотрены не были. Поэтому именно архитектура FIPA на данный момент пользуется большей популярностью.

В рамках проделанной работы были сформулированы основные требования к механизмам обеспечения информационной безопасности мультиагентной робототехнической системы на примере платформ, в основе которых лежит роевой алгоритм: необходимость идентификации и аутентификации агентов в системе, наличия системы защиты от компрометации криптоключей по побочным каналам, реализация системы ИБ с учетом ограниченности представления агентов обо всей системе, изменчивостью их пространственного положения и отсутствием централизации при роевой модели управления, обеспечение возможности выявления аномалий в действиях роя. Эти требования в дальнейшим должны учитываться при проектировании защищенной мультиагентной робототехнической системы.

В настоящее время отечественных стандартов спецификации агентных систем в нашей стране не создано. Вместе с тем вопросы стандартов коммуникации агентов в рамках мультиагентных робототехнических систем стоят достаточно остро.

Выбор протокола коммуникации, безопасного при организации мультиагентной системы различного уровня, различного подхода к организации внутрикомандного взаимодействия – это ключевая задача для проектировщика агентной системы.

Поэтому при проектировании любой агентной системы, прежде всего, необходимо сформулировать основные требования к протоколам коммуникации агентов любого уровня, отвечающих заданным параметрам безопасности. Задачей дальнейшей работы, таким образом, является выдвижение основных требований к спецификации протоколов коммуникации мультиагентных робототехнических систем, в том числе, с роевым интеллектом.

Лямзина А.Г., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ И ОСНОВНЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ПРОГРАММЫ «УМНЫЙ ГОРОД КРОНШТАДТ»

В современном мире стали активно использоваться самоорганизующиеся беспроводные сети, в частности, сенсорные сети. Сенсорная сеть — сеть множества датчиков (сенсоров), объединенных между собой посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счет способность ретрансляции сообщений от одного элемента к другому. В сенсорных сетях используются такие датчики, как: датчик температуры, датчик освещенности, датчик давления, датчик воды, и др. Зачастую сенсорные сети используются в системах «Умный дом».

В настоящее время проводятся разработки по созданию «Умных городов». Примером такого пилотного проекта в России стал город Кронштадт. Предполагаемой целью данного проекта является внедрение сенсорных сетей в каждую сферу жизнедеятельности города. Например, сенсоры, которые могут позволить оценить степень освещенности и включить или выключить систему уличного освещения; другим примером являются сенсоры, которые способны оценить загрузку мусорных контейнеров, и либо направить доп. мусоровозы, либо дать сигнал, что нет необходимости присылать автомобиль и таким образом сэкономить городу время, деньги; также система умной парковки, система видео наблюдения.

С 2013 года данная программа вступила в стадию реализации. В настоящее время над воплощением проекта работают предприятия радиоэлектронной промышленности Санкт-Петербурга во главе с ОАО "Авангард" совместно с Санкт-Петербургским Заводом имени Козицкого.

Разумеется, такая сложная система нуждается в необходимом и достаточном уровне защиты. Даже на этапе проектирования мы можем выявить набор уязвимостей и возможных угроз. В дальнейшей работе мы планируем, по возможности, досконально изучить топологию сети, основные характеристики устройств, составить модель угроз и нарушителя, и на основании этого постараться спроектировать возможную систему защиты и предложить её непосредственно разработчикам «Умного города Кронштадт».

Насретдинова Д.Р.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

УНИЧТОЖЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

На сегодняшний день современные организации и предприятия перенасыщены бумажной документацией, в связи с этим необходим регулярный контроль для хранения актуальной информации.

Экспертизу ценности документов необходимо проводить постоянно действующей экспертной комиссией. .

В процессе уничтожения конфиденциальных материалов должен быть установлен порядок, который исключает возможность изученияdокументов посторонними лицами.

В ходе уничтожения конфиденциальных документов могут возникнуть следующие угрозы: подмена документов, выделенных для уничтожения или изъятия из документов и дел отдельных частей (листов, фотографий, образцов печатей, росписей); ошибочного или умышленного выделения документов для уничтожения или фиктивное "уничтожение" ценных документов и дел; неполного уничтожения документов, дел и носителей, позволяющие восстановить их текст; утраты (утери, кражи) документов и дел, выделенных для уничтожения.

Состав необходимых документов для уничтожения письменно согласовывается и утверждается с руководителями подразделений или направлений деятельности. На всех этапах уничтожения документов, дел и других конфиденциальных материалов оформляется акт.

Процесс уничтожения конфиденциальных документов и носителей информации состоит из следующих процедур:

1.Подготовку документов, дел и носителей информации к уничтожению;

2.Оформление акта на уничтожение;

3.Уничтожение документов по акту.

Способы уничтожения бумажных документов:

- шредирование,
- сжигание,
- химическая обработка.

Каждый из перечисленных способов имеет свои положительные и отрицательные качества, и используется в зависимости от конкретного делопроизводства, законодательства и возможностей определенной организации.

Сжигание на протяжении многих лет было самым эффективным методом уничтожения бумажных документов. Основное достоинство данного метода — это его простота и дешевизна, при правильном применении гарантирует уничтожение информации, и, в крайнем случае, можно обойтись подручными средствами, без использования сложного дополнительного оборудования.

Одним из менее распространённых методов является химическая обработка. В процессе химической обработке совершаетсяразмягчение бумаги и превращение ее в бумажную массу. Это самый надежный, но недешевый метод, и в настоящее время его используют в качестве дополнительной меры безопасности при уничтожении секретных документов шредированием.

Шредирование — наиболее распространенный и популярный на сегодня метод уничтожения бумажных документов. Привлекают его дешевизна (и даже возможность заработать, сдавая бумажную обрезь в макулатуру), «экологичность», достаточная надежность.Организации или самостоятельно уничтожают документы, или пользуются услугами фирм, занимающихся переработкой вторичных отходов.

Таким образом, необходима четкая регламентация технологии уничтожения документов, дел и носителей информации, которая направлена, прежде всего, на исключение любой возможности утраты и подмены документов, предназначенных для уничтожения, неполного их уничтожения и последующего восстановления текста, а также предотвращения других опасностей для конфиденциальной информации.

Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ДЕСТРУКТИВНЫХ СОСТОЯНИЙ И ПЕРЕХОДОВ

В последнее время всё большее внимание уделяется вопросу защиты информационных систем (ИС), под которыми понимается совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. Риск-ориентированный, подход к выбору защитных мер для информационной системы обладает рядом преимуществ. Он позволяет экономически обосновать затраты на обеспечение безопасности ИС.

Вместе с тем, существует ряд проблем, затрудняющих использование риск-ориентированного подхода к выбору защитных мер.

Стоит отметить, что правила и процедуры оценки рисков сложно формализуются, поэтому оценка рисков чаще всего осуществляется с привлечением экспертов. Вследствие этого, динамическая детализированная оценка рисков безопасности ИС на сегодняшний день является очень трудоёмкой и трудновыполнимой.

Чаще всего, риск определяется как произведение трёх величин: вероятности возникновения угрозы, вероятности использования уязвимости и величины последствий.

Данный подход обладает рядом недостатков, связанных со сложность прогнозирования вероятности возникновения угроз и определением причинно-следственных связей между разными рисками.

В разработанной модели предлагается определять риск как произведение вероятности перехода компонента ИС в деструктивное состояние на величину возникающего при этом ущерба. За счёт этого удаётся избежать недостатков, указанных выше, вследствие того, что число деструктивных состояний, как и типов компонентов ИС, невелико, что позволяет установить причинно-следственные связи между переходами компонентов ИС в деструктивные состояния.

В то же время, состояние компонента ИС является внутренним по отношению к ИС, вследствие чего его проще спрогнозировать на основе имеющихся наблюдений и статистики.

Под деструктивным состоянием компонента ИС понимается нежелательное и незапланированное состояние компонента ИС, в котором он оказался в результате реализации одной или нескольких угроз. Определены множества деструктивных состояний для каждого из типов компонентов ИС:

- информационный актив (заблокирован, скомпрометирован, модифицирован);
- программное обеспечение (заблокировано, взломано, модифицировано);
- техническое средство (заблокировано, повреждено, утеряно, модифицировано);
- каналы данных (взломан, повреждён).

Под переходом понимается изменение состояния компонента информационной системы с нормального на деструктивное в результате реализации угрозы. Переход компонента ИС в деструктивное состояние может быть вызван действиями источника угроз, либо переходом другого, связанного компонента ИС в деструктивное состояние. Под источником угрозы

понимается субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации. Чаще всего выделяют стихийные, техногенные и антропогенные источники угроз.

Для каждого деструктивного состояния определяется функция вероятности перехода, принимающая значения в интервале [0,1] и зависящая от ряда параметров, к которым относятся:

– уязвимости компонентов ИС и элементов её непосредственного окружения;
– условия эксплуатации компонентов ИС;
– эффективность реализованных защитных мер.

Базовая модель оценки вероятности перехода разработана с участием группы экспертов. Предложен алгоритм обучения базовой модели на основе статистики инцидентов с использованием метода градиентного спуска.

Для определения величины последствий от перехода компонента ИС в деструктивное состояние для каждого типа компонентов ИС сформированы классификаторы последствий, учитывающий финансовые, репутационные, производственные, экологические, правовые и иные последствия.

Представленная модель оценки рисков безопасности ИС на основе состояний и переходов позволяет осуществлять динамическую итеративную оценку рисков без постоянного привлечения экспертов.

Также она позволяет установить взаимосвязи между рисковыми событиями (переходами компонентов ИС в деструктивные состояния), что даёт возможность проводить анализ различных сценарией реализации угроз.

Петрук Т.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИЗГИБ ОПТИЧЕСКОГО ВОЛОКНА КАК ОДИН ИЗ СПОСОБОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Волоконно-оптическая линия связи (ВОЛС) представляет собой систему передачи информации, основанную на использовании оптических диэлектрических волноводов, известных как «оптическое волокно». ВОЛС обладает рядом преимуществ, главным из которых принято считать защищенность от несанкционированного доступа, в сравнении, например, с кабельными линиями, которые на сегодня уже исчерпали свой ресурс развития. Поставленная задача заключается в глубоком анализе возможных каналов утечки информации (КУИ), изучении и предложении способов защиты.

Один из таких методов, на который стоит обратить внимание, это изгиб волокна. Именно он позволяет осуществить направленный вывод излучения, что не скажешь о других методах. Эффективность заключается в возможности изменения радиуса изгиба волокна в следствии чего достигается нужное количество получаемой мощности, вполне достаточной для перехвата информации.

В связи с возможностью компрометации передаваемых данных или их модификации нельзя обойтись без разработки методов защиты на основе квантовой криптографии, которая является перспективным направлением для защиты информации в ВОЛС.

Ральникова Н.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОПТИЧЕСКОЕ ТУННЕЛИРОВАНИЕ КАК МЕТОД ФОРМИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

В последнее время все большую популярность набирают волоконно-оптические линии связи (ВОЛС). ВОЛС представляет собой канал связи, основанный на использовании оптических диэлектрических волноводов, известных как "оптическое волокно". Само оптоволокно представляет собой прозрачную нить из стекла или пластика, которая переносит внутри себя свет посредством явления полного внутреннего отражения.

Долгое время считалось, что по причине отсутствия излучения организовать несанкционированный доступ в оптическом кабеле крайне сложно. Были известны лишь методы, предполагающие нарушение целостности оптоволокна, от которых достаточно легко защититься. Поэтому считалось, что оптоволоконные линии связи обладают очень высокой защищенностью от несанкционированного доступа. Но позже, после проведения некоторых исследований, стало ясно, что съем информации в ВОЛС возможен и без нарушения целостности волокна.

Один из таких методов НСД связан с отводом части светового потока из оптического волновода при нарушении полного внутреннего отражения. В идеальном случае свет не выходит из оптического волокна вследствие полного внутреннего отражения на его границах. Любые отклонения в распространении света приводят к выходу части излучения из волновода, которое образует канал утечки информации. Сформировать канал утечки данным методом можно разными вариантами: при

помощи механического, акустического или химического воздействия, тепловых колебаний, воздействия электрическими полями и при помощи оптического туннелирования. Остановимся подробнее на последнем из них.

Оптическое туннелирование позволяет захватывать часть электромагнитного излучения, выходящего за пределы сердцевины информационного оптического волокна дополнительным световодом, не внося дополнительных потерь и обратного рассеяния. Оно состоит в прохождении оптического излучения из среды с показателем преломления n1 через слой с показателем преломления n2 меньшим n1 в среду с показателем преломления n3 при углах падения, больших угла полного внутреннего отражения.

При распространении света в оптическом волокне часть светового потока выходит за пределы сердцевины оптоволокна. Интенсивность излучения вышедшего из сердцевины в оболочку оптоволокна на расстояние r в зависимости от угла падения на границе сердцевина-оболочка можно вычислить при помощи формулы.

При приближении угла падения к углу полного отражения показатель степени экспоненты стремится к нулевому значению, свет распространяется по всей структуре волокна – сердцевине и оболочке. Это приводит к тому, что часть интенсивности из основного оптоволокна может перейти в дополнительное оптоволокно.

Максимум значения коэффициента связи достигается при нулевом расстоянии между оболочкой и дополнительным оптоволокном и показателе преломления дополнительного волокна n3=n1.

Сформировать канал утечки данным способом из волокна в специальное волокно можно при помощи специального оптического соединителя, работающего на принципе оптического туннелирования. Примером такого оптического соединителя может служить механический соединитель оптических волокон Fibrlok II 2539.

Отличительной особенностью оптического туннелирования является отсутствие обратно рассеянного излучения, что затрудняет детектирование несанкционированного доступа к каналу связи. Этот способ съема информации наиболее скрытный.

На принципах оптического туннелирования в интегральной и волоконной оптике создаются такие устройства, как оптический ответвитель, оптофоны, волоконно-оптические датчики физических величин.

Несмотря на распространенное мнение о невозможности подключения к ВОЛС без нарушения целостности волокна, такие методы все же существуют. Формирование канала утечки информации, передаваемой по ВОЛС, при помощи оптического туннелирования – самый скрытный из таких методов. Это опровергает утверждение о невозможности формирования более менее скрытого канала утечки из оптического волновода. Однако, несмотря на это, оптическое волокно остается самой безопасной средой передачи информации на большие расстояния.

Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ОТКРЫТЫЕ ДАННЫЕ. ЭФФЕКТИВНОСТЬ И РЕЗУЛЬТАТИВНОСТЬ МЕР ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В связи с реализацией Концепции открытости органы исполнительной власти выкладывают открытые сведения, поскольку целью является улучшение системы государственного управления. Перед получением результатов по совершенствованию, встали вопросы повышения доверия к открытым данным, хранение данных для постобработки результатов использования, разработка методик разбора конфликтных ситуации при обязательном использовании открытых данных[1]. По достижение данных задач начали появляться проекты на основе анализа сведений предоставленных исполнительными органами власти, например, сопоставление рыночных цен лекарств в Москве[2] и открытых данных Министерства Здравоохранения предельных отпускных цен производителей на лекарственные препараты, включенные в перечень жизненно необходимых и важнейших лекарственных препаратов[3]. Следует учесть, что из-за большого интереса общества к анализу данных возникнут ошибочные результаты из-за ошибочных гипотез или методов анализа Больших данных. Поэтому с точки зрения безопасности информации необходимо создать критерий верификации гипотез, что направит начинающих (молодых) специалистов по анализу данных. В настоящей работе будут рассмотрены элементарные методы валидации результатов аналитических работ, в частности, проверка достоверности начальных сведений, частично используемых методов на основе используемых критериев и отборов к выборке и самому результату. Проверка достоверности начальных сведений необходим, поскольку пользователь открытых данных вправе адаптировать, модифицировать, что возможны ошибки. В применений могут возникнуть ошибки не только 1 рода, а также 2 рода, согласно математической статистики. Что с точки зрения безопасности нарушается

целостность информации. Который влечет нарушение дополнительных свойств такого как достоверность.

Чалыкин И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ СУБД «ORACLE»

В современном мире, пожалуй, каждая компания довольно быстро сталкивается с необходимостью централизованно хранить и обрабатывать информацию. Как правило, для этого применяются базы данных − в них может находиться практически любая текстовая информация, начиная от личных сообщений и статей, заканчивая диагнозами пациентов, персональными данными и номерами кредитных карт.

Сразу следует заметить, что по статистике на 2015 год наиболее популярной системой управления базами данных является «Oracle RDBMS», причем это касается абсолютно всех информационных систем. Если же рассмотреть финансовый сектор, то обычно ни один банк, ни один крупный платежный центр не обходится без данной базы данных. Данный факт подчеркивает актуальность и важность выбранной тематики работы. В ходе проведения исследования было отмечено, что, к сожалению, по умолчанию даже самая современная версия этой базы данных имеет достаточно низкий уровень информационной защищенности, а количество хакерских атак растет с каждым днем.

Целью данной работы является исследование недостатков существующих защитных механизмов и углубление знаний, связанных с предотвращением атак на систему управления базами данных «Oracle». В докладе будет рассмотрена типовая структура реляционной базы данных, архитектура и внутреннее устройство СУБД «Oracle». В ходе доклада будут рассмотрены следующие вопросы:

– как устроена база с точки зрения архитектуры
– какие возможны атаки со стороны внешнего периметра – атаки на сетевые сервисы
– какие уязвимости могут быть реализованы изнутри – в том случае, если нарушитель смог получить в руки учетные данные

В качестве рассматриваемых систем были использованы все доступные версии данной базы – устаревшие и достаточно редко встречаемые девятые-десятые, наиболее популярная одиннадцатая, и самая современная, двенадцатая.

Данный доклад будет полезен тем студентам, которые бы хотели начать изучать безопасность СУБД «Oracle», ознакомиться с основными известными атаками, а также методами защиты от них.

Шевченко Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

ВОССТАНОВЛЕНИЕ ИЗОБРАЖЕНИЙ МЕТОДОМ СЛЕПОЙ ДЕКОНВОЛЮЦИИ

Повсеместное распространение цифровых фотографий обуславливает актуальность задач восстановления цифровых изображений. Смаз при движении является дефектом, который приводит к появлению нечетких изображений и потере информации. Его причиной является движение датчиков камеры, захватывающих поступающий свет. Смазанное изображение может быть представлено в виде комбинации исходного изображения и смазывающего оператора – функции импульсного отклика. В таком случае задача восстановления смазанного изображения будет состоять из двух этапов: нахождение функции импульсного отклика и получение исходного изображения по найденной функции.

Операция применения искажающей функции к другой функции, например, к изображению, называется сверткой (конволюцией), т.е. некоторая область исходного изображения сворачивается в один пиксель искаженного изображения. Операция, обратная свертке, называется деконволюцией.

Существует несколько подходов к восстановлению изображений. При «неслепой» деконволюции ядро сдвига известно, и задача состоит в том, чтобы восстановить исходное изображение из искаженного, используя это ядро – классические линейные методы восстановления. Существует множество методов деконволюции, применяемых в такой ситуации, таких как обратная фильтрация, фильтр Тихонова, фильтр Винера, фильтрация методом наименьших квадратов, метод фильтрации Калмана-Бьюси. Во всех перечисленных методах предполагается, что искажающая функция точно известна, что в реальности не так. Во многих практических ситуациях количество информации о реальном изображении очень мало, ядро искажения можно определить лишь приблизительно по характеру видимых искажений. Поэтому исходное изображение должно быть восстановлено непосредственно из смазанного с использованием неполной информации о процессе смаза. Такие оценочные подходы, в которых модель искажения неизвестна, называются «слепой» деконволюцией. Методы слепого восстановления содержат много проблем, не имеющих

однозначного решения, поэтому в этой области возможно проведение многочисленных исследований.

Общий принцип слепой деконволюции достаточно простой – выбирается первое приближение искажающей функции, далее по одному из методов делается деконволюция, после чего некоторым критерием определяется степень качества, на основе нее уточняется функция искажения и итерация повторяется до достижения нужного результата. В большинстве методов слепой деконволюции частичная информация объединяется по оптимальным критериям, которые необходимо минимизировать. На данный момент не существует универсальных алгоритмов решения данной проблемы. Все алгоритмы или требовательны к ресурсам или обладают нехваткой надежности и стабильности.

Центральным вопросом при слепой деконволюции является выбор целевой функции, значение которой тем выше, чем ближе получаемый результат к желаемому. В качестве такой функции можно использовать распределение градиентов значений отдельных пикселей. Для резких изображений это распределение имеет пик в окрестности нуля и относительно слабое снижение вероятностей при приближении к большим значениям. При смазе же большие значения градиентов встречаются реже. Таким образом, в итерационной части алгоритма реконструкции изображения можно использовать распределение градиентов как меру приближения полученного изображения к реальному. На каждой итерации происходит уточнение ядра искажения путем решения задачи минимизации, затем на основе полученного ядра производится вычисление реконструированного изображения и определение необходимости дальнейших итераций.

Задача восстановления искаженных изображений актуальная во многих областях науки и техники, использование методов слепой деконволюции способно помочь в ее решении при отсутствии информации об искажающей функции.

Шоломов И.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

АКТУАЛЬНОСТЬ ИННОВАЦИОННОГО ПОДХОДА К АНАЛИЗУ СОСТОЯНИЙ ИБ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ, НА ОСНОВЕ КОМПЛЕКСИРОВАНИЯ ИНФОРМАЦИИ, ПОСТУПАЮЩЕЙ ОТ РАЗНОРОДНЫХ СЕНСОРОВ

Беспроводные сенсорные сети – это сети полупроводниковых сенсорных устройств, они долговечны, в силу потребления низкого количества энергии; гибки и устойчивы, при выходе из строя одного из устройств сеть продолжает функционировать; безопасны и дешевы в развертывании и эксплуатации, благодаря своей простоте, а также имеют неограниченную возможность расширения, встроенный интеллект настройки сети и маршрутизации.

Они могут использоваться, например, в системе «умный дом», а также для осуществления контроля над процессом производства на каком-либо предприятии, и, в конце концов, как средство для мониторинга за состоянием окружающей среды. На сегодняшний день существует и активно развивается проект «умного города» в Кронштадте. Но такое распространение сенсорных сетей, особенно в промышленном секторе, означает, что от их функционирования зависят жизни людей, и не только. По этой причине следует уделять большое внимание безопасности таких сетей.

К сожалению, не существует абсолютной защиты. Всегда есть шанс того, что злоумышленникам удастся добиться своих целей. Поэтому очень важно постоянно совершенствовать методы и средства обработки и защиты информации, особенно в таких новых областях, как беспроводные сенсорные сети. Наиболее популярной технологией в сфере беспроводных сенсорных сетей является ZigBee, однако уже было доказано, что у данной технологии существуют проблемы безопасности. В частности, было проведено исследование аномального поведения ZigBee-устройств, подвергающихся DOS-атаке, в результате которого были выявлены отклонения от нормального функционирования модулей беспроводной сенсорной сети при подобного рода атаках.

Говоря о том, что данный вид сетей является уязвимым, нужно помнить о том, что помимо защиты этой самой сети, необходим также постоянный мониторинг её состояния. Анализ траффика в таких сетях на сегодняшний день проводится самыми разнообразными способами: с применением SCADA систем, программными комплексами с передачей данных по стандартам IEEE 802.15.1 (Bluetooth) и IEEE 802.11 (Wi-Fi) и т.д. Анализ агрегируемого таким образом трафика может проводиться самыми разными методами, начиная от текстовой обработки с применением парсинга входных данных и заканчивая имитационным моделированием в режиме реального времени.

Автором данной работы были проанализированы открытые источники информации по существующим разработкам в данной области, проанализированы существующие подходы и средства анализа состояний информационной безопасности самоорганизующихся сетей, на основе комплексирования информации, поступающей от разнородных сенсоров.

Результатом написания данной работы стало более глубокое понимание автором предметной области и формирование мнения о том, в каком направлении стоит вести исследования и разработки

с целью увеличения эффективности применяемых методик анализа состояний информационной безопасности самоорганизующихся сетей, на основе комплексирования информации, поступающей от разнородных сенсоров.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ 15

Юсупов Р.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ ОТЕЧЕСТВЕННОЙ НАУКИ И ОБРАЗОВАНИЯ НА СОВРЕМЕННОМ ЭТАПЕ..... 15

Болгов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПОЛИТИКА РОССИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ 15

Бондуровский В.В., Вус М.А.
Россия, Санкт-Петербург, Секретариат Совета Парламентской Ассамблеи Организации Договора о коллективной безопасности, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ЗАКОНОДАТЕЛЬСТВО ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ ОДКБ..... 16

Алейник Я.А.
Россия, Санкт-Петербург, Группа компаний «Омега»
ИМПОРТОЗАМЕЩЕНИЕ. ВОЗМОЖНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ПЛАТФОРМЕ 1С: ПРЕДПРИЯТИЕ ПРИ ПОДКЛЮЧЕНИИ К ГИС - ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТАМОЖЕННЫХ ОРГАНОВ 17

Андреевский И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОСОБЕННОСТИ РАЗРАБОТКИ БЕЗОПАСНЫХ ПРИЛОЖЕНИЙ В ОБЛАКЕ ДЛЯ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ..... 17

Брысова В.А., Шубинский М.И.
Россия, Санкт-Петербург, Администрация Петроградского района, ИМЦ Петроградского района
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ШКОЛЫ НА ПРИМЕРЕ ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА 18

Волков Ю.Д.
Россия, Саранск, Мордовский государственный университет им. Н.П. Огарева
ИНТЕЛЛЕКТУАЛИЗАЦИЯ ЭКСПЕРИМЕНТА В АВТОНОМНЫХ ЭНЕРГОСИСТЕМАХ: ПРОБЛЕМНО-ОРИЕНТИРОВАННЫЙ ПОДХОД..... 19

Горелик С.Л., Лещинский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ЗАЩИТА ОТЧЕТНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННЫХ ИСКАЖЕНИЙ В СИСТЕМАХ УЧЕТА ПАССАЖИРСКОГО ТРАНСПОРТА 20

Горелик С.Л., Лещинский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПЕРЕВОЗКИ ПАССАЖИРОВ..... 21

Игнатьев М.Б., Легкий В.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМА ПОСТРОЕНИЯ УМНОГО БЕЗОПАСНОГО ГОРОДА С ПОЛИЦЕНТРИЧЕСКОЙ СТРУКТУРОЙ НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА 21

Лепёхин А.Н.
Республика Беларусь, Минск, Академия МВД Республики Беларусь
О НЕКОТОРЫХ МЕТОДАХ ОБРАБОТКИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 22

Присяжнюк С.П.,
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»
ПРИНЦИПЫ УПРАВЛЕНИЯ РЕГИОНОМ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОЙ ГИС 23

Присяжнюк С.П.
Россия, Санкт-Петербург, ЗАО «Институт Телекоммуникаций»
ГЕОИНФОРМАЦИОННАЯ ПЛАТФОРМА ДЛЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ РЕГИОНА 23

Степанов П.П.
Россия, Владивосток, Дальневосточный федеральный университет
АНАЛИЗ ПРОБЛЕМЫ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ 23

Томша П.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОЦЕНКА СТЕПЕНИ ВОВЛЕЧЕННОСТИ РЕГИОНАЛЬНЫХ ЗАКОНОДАТЕЛЬНЫХ ОРГАНОВ В РЕГУЛИРОВАНИЕ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 24

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 26

Алексеев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ АСПЕКТЫ ТЕХНОЛОГИИ СИНТЕЗА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА В ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ 26

Алексеев С.А., Горшкова Т.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ АСПЕКТЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ В ПОДРАЗДЕЛЕНИЯХ ОВД КАК СОЦИАЛЬНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМ 27

Бобонец С.А., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, Санкт-Петербургский университет МВД России
ПРИМЕНЕНИЕ ПРОЦЕДУР ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ 28

Богданов С.Д., Стурза К.И.
России, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОДНО ИЗ НАПРАВЛЕНИЙ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ 29

Большакова Л.В., Примакин А.И., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 30

Большакова Л.В., Примакин А.И., Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРИМЕНЕНИЕ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ 31

Большакова Л.В., Потехин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРИМЕНЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С КУРСАНТАМИ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 10.05.05 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ»..... 32

Борисов А.А.Толкачева Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВАЯ ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ 33

Буйневич М.В., Примакин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
КАТЕГОРИАЛЬНЫЙ АНАЛИЗ ПРОБЛЕМ ГАРМОНИЗАЦИИ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 34

Васильков В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПОЛИЦИИ» ОТ 7 ФЕВРАЛЯ 2011 ГОДА 35

Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОБЕСПЕЧЕНИЕ ПРОЦЕССА ОБУЧЕНИЯ КУРСАНТОВ ОСНОВАМ КРИПТОГРАФИИ 36

Вихман М.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ЗНАЧЕНИЕ КРИПТОЛОГИИ ДЛЯ ОВД 36

Вождаев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
АНАЛИЗ ПРАВОВОГО ОБЕСПЕЧЕНИЯ РОССИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 37

Вус М.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СОВЕРШЕНСТВОВАНИЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА О ГОСУДАРСТВЕННЫХ СЕКРЕТАХ 38

Зайцева Е.А., Морозов Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
К ВОПРОСУ ОБ УГОЛОВНО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИЗА РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙГОСУДАРСТВЕННУЮ ТАЙНУ 39

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРАВОВЫЕ АСПЕКТЫ ПОСТРОЕНИЯ WEB-САЙТОВ 41

Кононов О.А., Кононова О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРАВОВЫЕ ОСНОВЫ ОРГАНИЗАЦИИ ИНТЕРНЕТА 41

Макарова Е.Н., Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ О ПРАВОВОМ ОБЕСПЕЧЕНИИ КОНТРОЛЯ СЕТИ ИНТЕРНЕТ В РОССИИ 42

Морозов Н.М.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ НЕСЕРТИФИЦИРОВАННЫХ СРЕДСТВ СВЯЗИ В СИЛОВЫХ СТРУКТУРАХ 43

Нигметов Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВОПРОСОВ БЕЗОПАСНОСТИ СОДЕЙСТВИЯ ГРАЖДАН ОПЕРАТИВНО-РАЗЫСКНЫМ ОРГАНАМ 44

Парфенов Н.П.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ОСНОВА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА 45

Петрусевич Д.К.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
АНАЛИЗ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ КОММЕРЧЕСКОЙ ТАЙНЫ 46

Солодовник В.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
О НЕКОТОРЫХ ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 47

Суровенко И.А., Быстрова Н.С.
Россия, Санкт-Петербург, РОПД ГСУ ГУ МВД России по Санкт-Петербургу и Ленинградской области
РОЛЬ УГОЛОВНОГО КОДЕКСА В ОБЕСПЕЧЕНИИ ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 48

Томашевич Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЗАЩИТА И БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКА 48

Харрасов Э.Э.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 49

Яковлева Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ТЕСТОВОГО КОНТРОЛЯ ЗНАНИЙ КУРСАНТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ОПЫТ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ) 50

Якушев Д.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕРМИНОЛОГИЯ 51

Ярмоленко Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
СОСТОЯНИЕ И ВОЗМОЖНОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ 52

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 54

Абрамян Г.В.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А. И. Герцена
РИСКИ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ НА ПЛАТФОРМЕ WINDOWS НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ РОССИЙСКОЙ ФЕДЕРАЦИИ 54

Агеева Е.С., Прохоров А.И., Смагулова А.С., Золотарев В.В.
Россия, Красноярск, Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнёва
РАЗРАБОТКА МЕТРИЧЕСКОГО СПОСОБА КЛАССИФИКАЦИИ ПРОГРАММНОГО КОДА 55

Александров В.А., Десницкий В.А., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»
РАЗРАБОТКА И АНАЛИЗ ФРАГМЕНТА ЗАЩИЩЕННОЙ СИСТЕМЫ, РЕАЛИЗУЮЩЕЙ КОНЦЕПЦИЮ ИНТЕРНЕТ ВЕЩЕЙ 56

Барышникова Н.Ю., Егоров А.Н., Крупенина Н.В., Тындыкарь Л.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ЭЛЕКТРОННОГО ТЕСТИРОВАНИЯ ДЛЯ ОЦЕНКИ СООТВЕТСТВИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ РАБОТНИКОВ МОРСКИХ СПЕЦИАЛЬНОСТЕЙ 57

Бачурин И.В., Касаткин В.В., Лысенко В.А., Кузнецов А.Ю., Чендрова Ю.В., Сальникова П.Ю., Сычугов Д.С.
Россия, Архангельск, Агентство записи актов гражданского состояния Архангельской области
Санкт-Петербург, Объединенный учебно-методический совет по направлению «Информационные системы и технологии», Санкт-Петербургский государственный университет технологии и дизайна, ООО «Ультраполимеры», ЗАО «ЛюксофтПрофешонал»
Ростов-на-Дону, Ростовский государственный университет путей сообщения
БЕЗОПАСНОЕ WEB-ПРИЛОЖЕНИЕ ДЛЯ УПРАВЛЕНИЯ ИМУЩЕСТВЕННЫМ КОМПЛЕКСОМ УНИВЕРСИТЕТА 58

Бачурин И.В., Лысенко В.А., Чендрова Ю.В., Кузнецов А.Ю., Сычугов Д.С., Сальникова П.Ю.
Россия, Архангельск, Агентство записи актов гражданского состояния Архангельской области
Санкт-Петербург, Санкт-Петербургский государственный университет технологии и дизайна», ЗАО «Люксофт Профешонал», ООО «Ультраполимеры»
Ростов-на-Дону, Ростовский государственный университет путей сообщения
ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ПЛАТФОРМЕ IBM NOTES/DOMINO 59

Богданов Т.Р.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
УСТРАНЕНИЕ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В МОДУЛЕ ФОРМИРОВАНИЯ СТРУКТУР ДАННЫХ ПРИ ПРОВЕДЕНИИ ИССЛЕДОВАНИЯ 60

Браницкий А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МЕТОДЫ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ 61

Бурлов В.Г., Грачев М.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТУРЕ УПРАВЛЕНИЯ ВЫСШИМ УЧЕБНЫМ ЗАВЕДЕНИЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АНАЛИТИЧЕСКО-ДИНАМИЧЕСКОЙ МОДЕЛИ 62

БушуевС.Н., Чечулин А.А., Проноза А.А.
Россия, Санкт-Петербург, ЗАО «НПП «ТЕЛДА», Санкт-Петербургский институт информатики и автоматизации Российской академии наук
КЛАССИФИКАЦИЯ ИСТОЧНИКОВ ДАННЫХ О СЕТЕВЫХ ОБЪЕКТАХ И СВЯЗЯХ МЕЖДУ НИМИ 62

Волков В.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОЦЕССИНГОВЫЙ ЦЕНТР КАК ОСНОВА НАДЕЖНОСТИ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ 63

Гурьянов Д.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 64

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МОДЕЛЬ ПРОЦЕССА КОНФИГУРИРОВАНИЯ КОМПОНЕНТОВ ЗАЩИТЫ ВСТРОЕННЫХ УСТРОЙСТВ 65

Десницкий В.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МЕТОДИКА ОЦЕНКИ РЕСУРСОПОТРЕБЛЕНИЯ КОМПОНЕНТОВ ЗАЩИТЫ ВСТРОЕННЫХ УСТРОЙСТВ 66

Дешевых Е.А., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ОБЗОР СРЕДСТВ И ПЛАТФОРМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ ДЛЯ ЗАДАЧ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 67

Доброрадова В.А., Павлова Л.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПРОБЛЕМА АУТЕНТИФИКАЦИИ ОТКРЫТЫХ КЛЮЧЕЙ (ПРОБЛЕМА АУТЕНТИФИКАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ) 67

Дойникова Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРИМЕНЕНИЕ ГРАФОВ ЗАВИСИМОСТЕЙ СЕРВИСОВ В РАМКАХ ЗАДАЧИ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ ДЛЯ ОЦЕНИВАНИЯ КРИТИЧНОСТИ РЕСУРСОВ СИСТЕМЫ И ОБОСНОВАННОГО ВЫБОРА ЗАЩИТНЫХ МЕР 68

Дубровин Н.Д., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
РЕАЛИЗАЦИЯ ПРОТОТИПА НА БАЗЕ HADOOP ДЛЯ АНАЛИЗА БОЛЬШИХ ДАННЫХ 69

Дудка А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ВОЗМОЖНОСТЕЙ НАПРАВЛЕННОГО МИКРОФОНА И РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕР ПРОТИВОДЕЙСТВИЯ 70

Дудкина О.К., Копыльцов А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ЭТИЧНЫЙ ХАКЕР – НУЖНА ЛИ ТАКАЯ ПРОФЕССИЯ РОССИИ ТРЕТЬЕГО ТЫСЯЧЕЛЕТИЯ? 70

Дятлов О.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет технологии и дизайна
РАЗРАБОТКА XSLT-ШАБЛОНИЗАТОРА НА ОСНОВЕ ПРОТОТИПА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ ЗАЩИТЫ WEB-САЙТА 71

Евневич Е.Л.
Россия, Санкт Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПЕРСОНАЛИЗИРОВАННЫЙ СЕМАНТИЧЕСКИЙ ПОИСК И АНАЛИЗ СОМНИТЕЛЬНОГО КОНТЕНТА 71

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
СИНХРОННЫЙ МАГНИТНЫЙ УСКОРИТЕЛЬ МИКРОСПУТНИКОВ 72

Колодин М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРИМЕНЕНИЕ ЛЁГКОЙ ВИРТУАЛИЗАЦИИ И УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ ДЛЯ ОПТИМИЗАЦИИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ И НАДЁЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ 72

Коломеец М.В., Чечулин А.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ВИЗУАЛИЗАЦИЯ ПАРАМЕТРОВ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ С ПОМОЩЬЮ ДИАГРАММЫ ВОРОНОГО 73

Копыльцов А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ЛОКАЛЬНОЙ РЕГУЛЯЦИИ КРОВОТОКА 74

Копыльцов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОЦЕНИВАНИЕ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ 74

Крылов К.Ю., Ушаков И.А., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АНАЛИЗ МЕТОДИК ПРИМЕНЕНИЯ КОНЦЕПЦИИ БОЛЬШИХ ДАННЫХ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ 75

Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АРХИТЕКТУРАСИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В ПОМЕЩЕНИЯ НА ОСНОВЕ БЕСКОНТАКТНЫХ СМАРТ-КАРТ 76

Марков А.С., Фадин А.А.
Россия, Москва, ЗАО «НПО «Эшелон»
РЕАЛИЗАЦИОННЫЕ ОСНОВЫ СИГНАТУРНО-ЭВРИСТИЧЕСКОГО АНАЛИЗА БЕЗОПАСНОСТИ ПРОГРАММ 77

Михайлов Н.С.
Россия, Санкт-Петербург, АО «Равенство»
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ДОСТУПА В ПРОГРАММНЫЕ МОДУЛИ ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ 78

Михайлова А.С.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
СРЕДСТВА БЕЗОПАСНОГО ДОСТУПА ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТЕЗАУРУСА ТЕКСТОВОЙ ИНФОРМАЦИИ 78

Мондикова Я.А., Вайчикаускас М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОРГАНИЗАЦИЯ ОБМАННЫХ ЛОВУШЕК В АЛГОРИТМАХ ОТРИЦАЕМОГО ШИФРОВАНИЯ С РАЗДЕЛЯЕМЫМ СЕКРЕТНЫМ КЛЮЧОМ 78

Новикова Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ВИЗУАЛЬНЫЙ АНАЛИЗ ИЗМЕНЕНИЯ ПАТТЕРНОВ ДАННЫХ В ПОТОКАХ ДАННЫХ БОЛЬШОГО РАЗМЕРА 79

Новожилов Д.А., Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ПОДДЕРЖКИ ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТОВ ПО КЛАССИФИКАЦИИ ВЕБ-САЙТОВ 80

Первухина Е.Л., Осипов К.Н., Тимофеев И.
Россия, Севастополь, Севастопольский государственный университет
К ВОПРОСУ ИСПОЛЬЗОВАНИЯ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ УПРАВЛЕНИЯ ПРИЕМОСДАТОЧНЫМИ ИСПЫТАНИЯМИ ДВС 81

Проноза А.А., Чечулин А.А., Бушуев С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»
МОДЕЛЬ ПРЕДСТАВЛЕНИЯ ДАННЫХ РАЗНОРОДНОЙ СТРУКТУРЫ ОБ ИНФОРМАЦИОННЫХ ОБЪЕКТАХ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ ПОДСИСТЕМЫ ВИЗУАЛИЗАЦИИ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ И ИНФОРМАЦИЕЙ БЕЗОПАСНОСТИ 82

Рыжков С.Р.
Россия, Санкт Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ГЕОЛОКАЦИЯ ДЛЯ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ДАННЫХ 83

Саенко И.Б., Ганя С.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, ЗАО «НПП «ТЕЛДА»
ТЕХНИЧЕСКИЕ ПРИНЦИПЫ И МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОРГАНИЗАЦИИ И РАЗВЕРТЫВАНИЮ РЕШЕНИЙ ПО АГРЕГАЦИИ, НОРМАЛИЗАЦИИ, АНАЛИЗУ И ВИЗУАЛИЗАЦИИ БОЛЬШИХ МАССИВОВ ГЕТЕРОГЕННЫХ ДАННЫХ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ В СЕТЯХ «ИНТЕРНЕТ ВЕЩЕЙ» 84

Саенко И.Б., Котенко И.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА 85

Тындыкарь Л.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
АСПЕКТЫ ПРИМЕНЕНИЯ SCADA-ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И КОМПЛЕКСОВ 86

Федорченко А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРАВИЛО-ОРИЕНТИРОВАННЫЙ МЕТОД КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ 86

Федотов Е.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОДХОД К ФОРМИРОВАНИЮ ПАТТЕРНОВ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ 87

Ханыков И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СОПОСТАВЛЕНИЕ ДВУХ МЕТОДОВ АВТОМАТИЧЕСКОЙ СЕГМЕНТАЦИИ 88

Харинов М.В., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН
МОДЕЛЬ КВАЗИОПТИМАЛЬНОЙ СЕГМЕНТАЦИИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ 89

Чечулин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МАТЕМАТИЧЕСКИЕ МОДЕЛИ И АЛГОРИТМЫ МОДЕЛИРОВАНИЯ АТАК И ВЫРАБОТКИ КОНТРМЕР В РЕЖИМЕ, БЛИЗКОМ К РЕАЛЬНОМУ ВРЕМЕНИ 90

Шаповалов П.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОТОКОЛЫ ПОРОГОВОГО ОТРИЦАЕМОГО ШИФРОВАНИЯ 91

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ОЦЕНКА РИСКОВ УТЕЧКИ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИИ ПРИ ЭКСПОРТЕ ПРОДУКЦИИ ДВОЙНОГО НАЗНАЧЕНИЯ 91

Шишкин В.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СИМПТОМЫ, СИНДРОМЫ И УГРОЗЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 92

Шкарбан А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
МОНИТОРИНГОВЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ НА БАЗЕ МУЛЬТИАГЕНТНОГО ПОДХОДА 93

Щиголева М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОСТРОЕНИЕ МОДЕЛИ БЕЗОПАСНОЙ БИОТОПОЛОГИИ ДВИГАТЕЛЬНОЙ НАГРУЗКИ 93

Щиголева М.А., Виноградов А.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МЕТОДИКА БЕЗОПАСНОГО ЗОНИРОВАНИЯ ДЛЯ МОДЕЛИ ДВИГАТЕЛЬНОЙ НАГРУЗКИ 94

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
ИЗОБРАЗИТЕЛЬНАЯ КИБЕРНЕТИКА. СИСТЕМНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ ТЕХНОЛОГИЧЕСКОЙ ДИСЦИПЛИНЫ ДИЗАЙН 95

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 96

Аванесов М.Ю.
Россия, Санкт-Петербург, ЗАО «Институт Телекоммуникаций»
УПРАВЛЕНИЕ ПОТОКАМИ ДАННЫХ В МОБИЛЬНЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ ПОВЫШЕННОЙ ЖИВУЧЕСТИ 96

Бабаджанян Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
НОВЫЕ АЛГОРИТМЫ ДЛЯ ТЕХНОЛОГИИ МНОГОУРОВНЕВОГО ШИФРОВАНИЯ 97

Белоусов А.С., Ныркov А.П.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ МЕТОДАМИ ВИРТУАЛЬНОГО СЕГМЕНТИРОВАНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ 98

Биричевский А.Р.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СПОСОБ ПРИМЕНЕНИЯ ОТРИЦАЕМОГО ШИФРОВАНИЯ ДЛЯ ХРАНЕНИЯ КЛЮЧЕЙ 98

Брагина Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
СОВРЕМЕННЫЕ СРЕДСТВА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ 99

Брагина Е.К., Соколов С.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ОБЗОР ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ АНТИВИРУСНЫХ КОМПЛЕКСОВ.... 99

Булина А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
О ПРОБЛЕМЕ ВНЕДРЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО КОДА НА WEB-САЙТАХ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ: НЕЙТРАЛИЗАЦИЯ ПРОБЛЕМЫ..... 100

Галанов А.И., Березин А.Н., Синёв В.Е.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОТОКОЛ УТВЕРЖДАЕМОЙ ГРУППОВОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ДВУХ ТРУДНЫХ ЗАДАЧ..... 101

Горелочкина И.В., Белоусов А.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ЭЛЕКТРОННЫЕ СИСТЕМЫ ДОКУМЕНТООБОРОТА КАК СРЕДСТВО ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 102

Домбровская Л.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ХАРАКТЕРНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОВД 103

Ефимова А.Б.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России
ЗАЩИТА ИНФОРМАЦИИ В ВЫСШИХ ВОЕННО-ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ..... 104

Жуковский Е.В., Москвин Д.А., Зегжда Д.П.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого»
ПРИМЕНЕНИЕ АНАЛИЗА ЭНЕРГОПОТРЕБЛЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ ПРОГРАММНО-АППАРАТНЫХ ЗАКЛАДОК В ОБОРУДОВАНИИ КОМПЬЮТЕРА 105

Зыков В.М.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ПРИМЕНЕНИЕ ЭЛЕКТРОННЫХ КЛЮЧЕЙ..... 106

Иванов Д.В., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ИСПОЛЬЗОВАНИЕ КОНЦЕПЦИИ УПРАВЛЕНИЯ ПОТОКАМИ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ИНТЕЛЛЕКТУАЛЬНОГО ОКРУЖЕНИЯ..... 107

Игнатов Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ЭЛЕКТРОННАЯ ПОДПИСЬ КАК СРЕДСТВО ЗАЩИТЫ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ 107

Игнатьев М.Б., Попов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСПЕТЧЕРИЗАЦИИ ПОЛЕТОВ САМОЛЕТОВ В ЗОНЕ АЭРОПОРТА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ «ВИРТУАЛЬНАЯ БАШНЯ» 108

Игнатьев М.Б., Кузьмин Д.В., Попов Ю.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПАТТЕРНЫ ПОВЕДЕНИЯ ШЕСТИНОГО РОБОТА ПРИ ПЕРЕМЕЩЕНИИ ПО ПЕРЕСЕЧЕННОЙ МЕСТНОСТИ 108

Игнатьев М.Б., Жаринов О.О., Липинский Я.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ГАЗОПРОВОДОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АВТОНОМНОГО ШАГАЮЩЕГО АДАПТИВНОГО РОБОТА ДЛЯ ВНУТРИТРУБНОЙ ДИАГНОСТИКИ 109

Игнатьев М.Б., Попов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
БЕЗОПАСНОСТЬ ДОРОЖНОГО ДВИЖЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ АВТОМОБИЛЕЙ БЕЗ ВОДИТЕЛЕЙ 109

Когтев А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
СОВРЕМЕННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 109

Лаврова Д.С., Печенкин А.И.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ КОРРЕЛЯЦИОННО-РЕГРЕССИОННОГО АНАЛИЗА 110

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ПРАКТИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ 110

Лившиц И.И., Маликов В.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СОВРЕМЕННЫЕ РИСК-ОРИЕНТИРОВАННЫЕ СТАНДАРТЫ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ 112

Макарова Е.Н., Горбунова Е.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОЦЕССЕ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ 113

Марков В.С., Сидоренко Т.В.
Россия, Санкт-Петербург, Санкт-Петербургский научный Центр Российской академии наук
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ 114

Молдовян А.А., Березин А.Н., Михтеев М.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ОТРИЦАЕМОЕ ШИФРОВАНИЕ НА ОСНОВЕ СТАНДАРТНОЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ 115

Молдовян Н.А., Березин А.Н., Муравьёв А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОТОКОЛ ШИФРОВАНИЯ НА ОСНОВЕ ДВУХ ТРУДНЫХ ЗАДАЧ ПО КЛЮЧУ МАЛОГО РАЗМЕРА..... 116

Морозов В.Е., Дрозд А.В.
Россия, Москва, ООО «Новые Поисковые Технологии»
ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО КОМПЛЕКСА «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM» ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ ИЗ КОРПОРАТИВНЫХ СЕТЕЙ И КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В ОРГАНИЗАЦИИ..... 117

Нечитайленко Р.А., Лопаченок С.Б., Новопашин В.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОНЦЕПЦИЯ БЕЗОПАСНОСТИ СТЕК ТЕХНОЛОГИЙ ВЕБ-СЕРВИСОВ..... 118

Радченко Н.В., Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ОПЫТ ИССЛЕДОВАНИЯ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ПРИ ТЕСТИРОВАНИИ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОДА 120

Редковников В.А.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД 121

Рыжков А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ШИФРОВАНИЕ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ПО РАЗДЕЛЯЕМОМУ КЛЮЧУ МАЛОГО РАЗМЕРА 121

Смирнова О.Г., Хитов С.Б.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России, Санкт-Петербургский университет ГПС МЧС России
АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СПОСОБ РАЗРАБОТКИ ЭФФЕКТИВНЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ..... 123

Солодянников А.В., Пилипов М.В., Парамонов А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРИМЕТРА АВТОМАТИЗИРОВАННЫХ КАРТОГРАФИЧЕСКИХ СИСТЕМ..... 124

Марков А.С., Фадин А.А., Цирлов В.Л., Рауткин Ю.В.
Россия, Москва, ЗАО «НПО «Эшелон»
О ЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ..... 124

Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
К ВОПРОСУ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЪЮТЕРНОЙ ИНФОРМАЦИИ 125

Ныркov А.П., Черняков А.В.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
АЛГОРИТМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ 126

Яковлев А.Е.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПЕРЕХВАТ АУДИОИНФОРМАЦИИ С ПОМОЩЬЮ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ КАК ОДИН ИЗ ЭФФЕКТИВНЫХ ПУТЕЙ НЕГЛАСНОГО ПОЛУЧЕНИЯ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ 127

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 129

Авраменко В.С., Горячев С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОРГАНИЗАЦИЯМЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 129

Агеев С.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДЫ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ УПРАВЛЕНИЯ ЗАЩИЩЁННЫМИ МУЛЬТИСЕРВИСНЫМИ СЕТЯМИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ НЕЧЁТКОГО ВЫВОДА 129

Аксенов С.С., Лощенин Д.Е., Кий А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
К ВОПРОСУ ОБ АНАЛИЗЕ ЗАЩИЩЕННОСТИ ОПЕРАЦИОННЫХ СИСТЕМ 130

Аксенов С.С., Гурьев С.Н., Кочкин В.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В ЛВС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 131

Алашеев В.В.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
СИСТЕМНЫЙ ПОДХОД ВЫБОРА УГРОЗЫ СЪЕМА ИНФОРМАЦИИ 132

Анисимов В.В., Стародубцев Ю.И., Чукариков А.Г.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ПРЕВЕНТИВНОЙ ЗАЩИТЫ ИТКС СН, ИСПОЛЬЮЗУЮЩЕЙ РЕСУРСЫ ЕСЭ РФ 132

Анистратов И.В., Калюка В.И., Мешков И.С., Овсянников С.Н.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
Санкт-Петербург Военная академия связи имени Маршала Советского Союза С.М. Буденного, войсковая часть 25522
КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА WiMAX В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ 133

Байбиков Г.Р., Пицун А.Л.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ТРЕНАЖЕРОВ В ПРОЦЕССЕ ИЗУЧЕНИЯ ПРОГРАММ ПО ЗАЩИТЕ ИНФОРМАЦИИ 134

Банный Э.С.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
ТАЙНА ПЕРЕПИСКИ, ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ, ПОЧТОВЫХ, ТЕЛЕГРАФНЫХ И ИНЫХ СООБЩЕНИЙ 134

Бардюков Д.А., Подчасов О.П., Чернов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СПОСОБ СКРЫТОЙ ПЕРЕДАЧИ СООБЩЕНИЙ ИСТОЧНИКОВ ВИДЕОИНФОРМАЦИИ НА ОСНОВЕ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТЫХ КАНАЛОВ СВЯЗИ 135

Борисенко К.А., Бекенева Я.А., Шоров А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
СИСТЕМА МОДЕЛИРОВАНИЯ ДЛЯ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ ТЕХНИК БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ОТ DDOS-АТАК 136

Брунилин А.А., Куваев В.О., Петухов А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СЕМАНТИЧЕСКИЙ ПОДХОД ПРИ РЕШЕНИИ ОТДЕЛЬНЫХ ВОПРОСОВ РАЗГРАНИЧЕНИЯ ДОПУСКА ДОЛЖНОСТНЫХ ЛИЦ К ОБРАБОТКЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА 137

Бударин Э.А., Гелметдинов М.И., Столяров А.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДИКА ОЦЕНКИ СТРАТЕГИИ РАСПРЕДЕЛЕНИЯ СРЕДСТВ РАДИОПОДАВЛЕНИЯ ПО ЭЛЕМЕНТАМ СИСТЕМЫ РАДИОСВЯЗИ 137

Бунин А.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ЭТАПЫ РАЗРАБОТКИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 138

Бунин А.Б., Пантюхин О.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИМИТАЦИОННАЯ МОДЕЛЬ ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С БАЗОЙ ДАННЫХ 139

Вартанова Е.Ю.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 140

Васюков Д.Ю.,. Лаута О.С, Ефаров, И.А., Лаута А.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНЫХ АТАК 140

Винокуров А.В.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
СИСТЕМНЫЕ ИССЛЕДОВАНИЯ ВЫБОРА И ОБОСНОВАНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА И КРИТЕРИЕВ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ 141

Воронков К.Л., Труфанов С.К.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
РЕТРОСПЕКТИВНЫЙ АНАЛИЗ ДАННЫХ МОНИТОРИНГА СОБЫТИЙ БЕЗОПАСНОСТИ 141

Воронков К.Л., Таран В.В. Шерстюк Ю.М.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ СРЕДСТВ УПРАВЛЕНИЯ С ТЕЛЕКОММУНИКАЦИОННЫМ ОБОРУДОВАНИЕМ 142

Вотинов М.Л., Ковайкин Ю.В., Пичугин Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРИЧИНЫ ВОЗМОЖНОЙ УТЕЧКИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ ИЗ ОВ ВОЛС 143

Вотинов М.Л., Ковайкин Ю.В., Титова И.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРИМЕНЕНИЕ КВАНТОВОЙ КРИПТОГРАФИИ В ТКС 144

Газин А.В., Шубадеев А.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 144

Гусенцова П.Г., Закалкин П.В., Кузнецов С.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕШЕНИЯ ЗАДАЧИ КОНТРОЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ 145

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
МОДЕЛЬ ПРОЦЕССА КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ 146

Дементьев В.Е., Коцыняк М.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОДХОД К ОЦЕНКЕ ПРОТОКОЛЬНОЙ ЗАЩИЩЕННОСТИ ИТКС 147

Денисенко А.С., Куликов В.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛИРОВАНИЕ СУБД КАК СИСТЕМЫ С МАССОВЫМ ОБСЛУЖИВАНИЕМ 147

Денисенко А.С., Куликов В.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВЫБОР ПОКАЗАТЕЛЕЙ КАЧЕСТВА СУБД ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 148

Долгая А.А., Шункова И.Ю., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ДАННЫХ 149

Егоров А.Н., Кузнецов В.А.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМА ВОССТАНОВЛЕНИЯ ДОСТУПА К ДАННЫМ В КОРПОРАТИВНЫХ СЕТЯХ 149

Елизаров В.В., Паращук И.Б., Салюк Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного, ОАО «ИНТЕЛТЕХ»
АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ПРИМЕНЕНИЮ СРЕД И ТЕХНОЛОГИЙ РАЗРАБОТКИ ПРОГРАММНЫХ ПРОДУКТОВ В ИНТЕРЕСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 150

Емелин В.И., Подолянец Д.В.
Россия, Санкт-Петербург, ОАО «НИИ Вектор»
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАУКОЕМКИХ ТЕХНОЛОГИЙ РАДИОЭЛЕКТРОННОГО МОНИТОРИНГА НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА..... 151

Жигадло В.Э.
Россия,Санкт-Петербург, ООО «Симпл Групп»,
КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕРРИТОРИЯМИ «БЕЗОПАСНАЯ ТЕРРИТОРИЯ» 152

Жигадло В.Э.
Россия,Санкт-Петербург, ООО «Симпл Групп»
ПРОБЛЕМЫ СОЗДАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ СИТУАЦИОННЫХ ЦЕНТРОВ, КАК ЭЛЕМЕНТОВ СИСТЕМ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ 152

Жигадло В.Э.
Россия, Санкт-Петербург, ООО «Симпл Групп»
ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ РЕГИОНАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ 153

Жигадло В.Э.
Россия,Санкт-Петербург, ООО «Симпл Групп»,
ПРОБЛЕМЫ СОЗДАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ РЕГИОНАЛЬНЫХ МОНИТОРИНГОВЫХ ЦЕНТРОВ, КАК ЭЛЕМЕНТОВ СИСТЕМ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ. 153

Закалкин П.В., Кузнецов С.И., Сухорукова Е.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ЗАДАЧА МОНИТОРИНГА СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ..... 154

Закалкин П.В., Сухорукова Е.В., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ЗАЩИТА НАЦИОНАЛЬНОЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ КИБЕРВОЗДЕЙСТВИЙ..... 155

Зегжда Д.П., Зегжда П.Д., Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ ПРИ ПОСТРОЕНИИОТЕЧЕСТВЕННОЙ УНИВЕРСАЛЬНОЙ ЗАЩИЩЕННОЙ СЕТЕВОЙ УПРАВЛЯЮЩЕЙ ПЛАТФОРМЫДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРУПНОМАСШТАБНЫХ СЕТЯХС ДИНАМИЧЕСКОЙ ИНФРАСТРУКТУРОЙ 156

Израилов К.Е.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
ПОИСК УЯЗВИМОСТЕЙ В РАЗЛИЧНЫХ ПРЕДСТАВЛЕНИЯХ ПРОГРАММНОГО КОДА..... 157

Ищенко Д.В., Деньжонков К.А., Денисенко А.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 158

Калинин М.О., Минин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ В MESH-СЕТЯХ С ПОМОЩЬЮ АЛГОРИТМОВ SOFT COMPUTING..... 158

Калинин М.О.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ ВИРТУАЛЬНЫЙ КЛАСТЕР КАК УНИВЕРСАЛЬНАЯ ПЛАТФОРМА ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ШИРОКОПОЛОСНЫХ СЕТЯХ 159

Кий А.В., Логинов В.А., Лощенин Д.Е.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБ ИЗБЫТОЧНОСТИ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ПОДХОДЕ К ЕЕ СНИЖЕНИЮ 160

Ковриченков С.В., Кузнецов С.И., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ 160

Ковриченков С.В., Кузнецов С.И., Тесля С.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
НАПРАВЛЕНИЯ СОЗДАНИЯ ЕДИНОГО МЕХАНИЗМА БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ 161

Кораблин В.О.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
ОПЕРАТИВНАЯ ОБРАБОТКА ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИЙ 162

Корниенко Е.А., Кревная А.И., Стародубцев Ю.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
О ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ 163

Кочкин В.А., Хилько В.О., Аксенов С.С.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СИСТЕМЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ С ГИБРИДНОЙ РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ 164

Коцыняк М.А., Лаута О.С., Шаров И.А., Сабан М.Ю., Хорошков М.Э.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПЕРСПЕКТИВНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И СВЯЗИ И ПУТИ ИХ СОЗДАНИЯ 164

Коцыняк М.А., Лаута О.С., Корень М.Ю., Сабан М.Ю., Нечепуренко А.П.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 165

Кречин И.В., Бунин А.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИС 165

Куваев В.О.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛЬ ИНТЕГРАЦИИ СХЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА РАЗЛИЧНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ 166

Лазаро Зеферино, Грака Жозе Да Сильва, Митрофанов М.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.... 167

Лаута О.С., Баленко А.А., Лаута А.С., Лянгузов Д.А., Лукина О.М.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
КИБЕРУСТОЙЧИВОСТЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 168

Левоневский Д.К., Фаткиева Р.Р.
Россия, Санкт- Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ИЗМЕРЕНИЕ КРИТИЧЕСКИХ ХАРАКТЕРИСТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ 168

Лепешкин О.М., Бурлов В.Г., Алексеев С.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ 169

Лепешкин О.М., Морозов М.М., Чернов Д.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
РАЗРАБОТКА ФУНКЦИОНАЛЬНО-РОЛЕВОЙ МОДЕЛИ ДОТУПА 170

Логинов А.А., Кораблин В.О.
Россия, Санкт-Петербург, ЗАО «Институт инфотелекоммуникаций»
УНИФИКАЦИЯ СРЕДСТВ СБОРА ДАННЫХ СОБЫТИЙНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИЙ..... 170

Молдовян А.А., Ковцур М.М.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
ОЦЕНКА СКОРОСТНЫХ ХАРАКТЕРИСТИК РЕАЛИЗАЦИИ АТАКИ ТИПА ПЕРЕБОР ПАРОЛЯ НА IP-АТС ПРИ ИСПОЛЬЗОВАНИИ FAIL2BAN 171

Молтянинов А.К., Москаленко К.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБОСНОВАНИЕ ПО РЕАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ МНОГОАГЕНТНОЙ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЯМИ СВЯЗИ 172

Москаленко К.Н., Молтянинов А.К.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБОСНОВАНИЕ ПРОБЛЕМЫ ПО УПРАВЛЕНИЮ СЛОЖНЫМИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ 172

Овчаренко М.В., Винокуров А.В.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
МЕТОД КОМПЛЕКСНОЙ ОБРАБОТКИ ИНФОРМАЦИИ В АППАРАТУРЕ ПЕРЕДАЧИ ДАННЫХ..... 173

Олимпиев А.А.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
АТРИБУТНАЯ И РОЛЕВАЯ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА К ОБЪЕКТНОЙ МОДЕЛИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 173

Павленко Е.Ю., Москвин Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский политехнический университет Петра Великого
ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ДЕЦЕНТРАЛИЗОВАННЫХ СЕТЕЙ НА ОСНОВЕ АНАЛИЗА ПОТОКОВ ПЕРЕДАЧИ СЕТЕВОГО ТРАФИКА 174

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОБЛЕМЫ БОЛЬШИХ ДАННЫХ. ОСОБЕННОСТИ И ПУТИ РЕШЕНИЯ 175

Паращук И.Б.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОКАЗАТЕЛИ ДОСТУПНОСТИ ЛЕГАЛЬНЫХ (АВТОРИЗИРОВАННЫХ)ПОЛЬЗОВАТЕЛЕЙ К ЗАЩИЩАЕМОМУ ИНФОРМАЦИОННОМУ РЕСУРСУ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 176

Паращук И.Б., Порецков О.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПАРАМЕТРЫ ЦЕЛОСТНОСТИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 176

Пицун А.Л., Байбиков Г.Р.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ И ПУТИИХ РЕШЕНИЯ 177

Репников А.Ю., Худайназаров Ю.К., Штаненко В.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
КОНТРОЛЬ В ПРОБЛЕМАТИКЕ ЗАЩИТЫ СИСТЕМЫ СВЯЗИ ОТ РАДИОРАЗВЕДКИ 178

Рожнов М.Д., Мач Д.П., Шерстюк М.Ю.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
ФИЛЬТРАЦИЯ СОБЫТИЙ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 178

Рыбин П.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ КОМПЛЕКСОМ ПРИГОТОВЛЕНИЯ МНОГОКОМПОНЕНТНЫХ СМЕСЕЙ 179

Савельев И.Л., Шерстюк Ю.М.
Россия, Санкт-Петербург, ОАО «НИИ «Рубин»
УСТОЙЧИВОСТЬ И БЕЗОПАСНОСТЬ ТЕХНОЛОГИЧЕСКОГО МОНИТОРИНГА СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ 180

Сазонов В.В., Титов В.С., Зубакин В.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ПОВЫШЕНИЕ СТРУКТУРНОЙ СКРЫТНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С ХАОТИЧЕСКИМИ СИГНАЛАМИ 181

Синещук М.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России
ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ МЧС РОССИИ 182

Синещук Ю.И.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
КИБЕРБЕЗОПАСНОСТЬ И ПРОБЛЕМЫ ОПЕРАТИВНОЙ АДАПТАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ МВД РОССИИ. 183

Синюк А.Д., Остроумов О.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МЕТОДОЛОГИЯ ОТКРЫТОГО КЛЮЧЕВОГО СОГЛАСОВАНИЯ СЕТИ ТРЕХ КОРРЕСПОНДЕНТОВ 184

Синюк А.Д.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
МОДЕЛЬ БЕЗОПАСНОГО ФОРМИРОВАНИЯ СЕТЕВОГО КЛЮЧА..... 184

Сныткин И.И., Кулюпин Е.Н.,
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армииС.М. Штеменко
РЕАЛИЗАЦИЯ МЕХАНИЗМА И УСЛУГ ЗАЩИТЫ ИНФОРМАЦИИ (ШИФРОВАНИЕ ПОТОКА ТРАФИКА СОГЛАСНО ГОСТ РИСО 7498) НА 1-М УРОВНЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ ISO НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СИСТЕМНЫХ СВОЙСТВ И ХАРАКТЕРИСТИК ПРОИЗВОДНЫХ УПРАВЛЯЮЩИХ ЧИСЛОВЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ 185

Сныткин И.И., Кулюпин Е.Н., Сныткин Т.И.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Москва, 27 Центральный научно-исследовательский институт Министерства обороны Российской Федерации
НЕКРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СПОСОБЫ РЕАЛИЗАЦИИ МЕХАНИЗМОВ И УСЛУГ ЗАЩИТЫ ИНФОРМАЦИИ В ТРАНСПОРТНОЙ ПОДСИСТЕМЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ 186

Сныткин И.И., Кулюпин Е.Н., Сныткин Т.И.
Россия, Краснодар, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Москва, 27 Центральный научно-исследовательский институт Министерства обороны Российской Федерации
МЕТОД УСКОРЕННОГО ПРИЕМА И СИНХРОНИЗАЦИИ ПРОИЗВОДНЫХ НЕЛИНЕЙНЫХ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ КАК «ТРЕТЬЯ РЕШАЮЩАЯ СХЕМА» ЭФФЕКТИВНОГО РАДИОПРИЕМА..... 187

Суконщиков А.А., Яковлев С.А.
Россия, Вологда, Вологодский государственный технический университет,
Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
СИТУАЦИОННОЕ ИНТЕЛЛЕКТУАЛЬНО-АГЕНТНОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ..... 188

Таран В.В., Шерстюк К.Ю., Шерстюк Ю.М.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
ФУНКЦИОНАЛЬНЫЕ ПОДСИСТЕМЫ И ПРОФИЛИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В АСУС 188

Труфанов С.К.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
ПОИСК ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПО ДАННЫМ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИЙ 189

Удалов В.С., Гаскаров В.Д.
Россия, Санкт-Петербург, ФБУ «Администрация «Волго-Балт», Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СУДОПРОПУСКА ЗА СЧЕТ ИНТЕРГАЦИИ СИСТЕМ ПОЗИЦИОНИРОВАНИЯ И ВИДЕОНАБЛЮДЕНИЯ..... 190

Фаткиева Р.Р.
Россия, Санкт Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АВТОМАТИЗАЦИЯ ВЫБОРА ПОКАЗАТЕЛЕЙ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ..... 191

Фёдоров В.Г., Стародубцев Ю.И.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ЗАДАЧА КЛАССИФИКАЦИИ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ 191

Хритинин В.В., Чирушкин К.А., Ковальченко Д.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
УГРОЗЫ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВОЕННОЙ АКАДЕМИИ СВЯЗИ 192

Чеснаков М.Н., Латушко Н.А., Карпов А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ТРЕБОВАНИЯ К ОПЕРАТОРАМ СВЯЗИ ЕДИНОЙ СЕТИ ЭЛЕКТРОСВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПРЕДОСТАВЛЯЮЩИМ УСЛУГИ СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ 193

Шерстюк М.Ю.
Россия,Санкт-Петербург,ЗАО«Институтинфотелекоммуникаций»
ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ УЧЕТНЫХ ДАННЫХ В АСУС В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 193

ШубадеевА.С., ЛогиновВ.А., Кий А.В., Газин А.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
СОДЕРЖАНИЕ ПЛАНИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ 194

Шустров Е.С., Шустрова Е.Ю., Иванцов Е.В.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Москва, в/ч 52686
ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМОВ УПРАВЛЕНИЯ МАРШРУТИЗАЦИЕЙ В СЕТИ ПЕРЕДАЧИ ДАННЫХ..... 195

Яцков А.В., Столяров А.Н.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
АЛГОРИТМ ЦЕНТРАЛИЗОВАННОГО ЦЕЛЕРАСПРЕДЕЛЕНИЯ В СИСТЕМАХ РАДИОПОДАВЛЕНИЯ 196

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ 197

Алексанков С.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МОДЕЛЬ ДИНАМИЧЕСКОЙ МИГРАЦИИ ВИРТУАЛЬНЫХ МАШИН 197

Аминов Х.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКАХ..... 197

Байковский В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОБЛЕМЫ БЕЗОПАСНОСТИ СЕТИ IP-ТЕЛЕФОНИИ ДЛЯ НАУЧНО-ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ 198

Безрук Г.Г., Левкин И.М.
Россия, Санкт-Петербург, НИИО МРТ ФГБУ ГНИИЦ РТ МО РФ, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОБОБЩЕННЫЕ КОМПЛЕКСНЫЕ ПАРАМЕТРЫ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ 198

Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОПТИМИЗАЦИЯ СТРУКТУРЫ И ПРОЦЕССА ПЕРЕРАСПРЕДЕЛЕНИЯ ЗАПРОСОВ В МУЛЬТИКЛАСТЕРНЫХ СИСТЕМАХ 199

Богатырев В.А., Богатырев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИОННЫХ УСЛУГРЕАЛЬНОГО ВРЕМЕНИ В УСЛОВИЯХ ОШИБОК, ОТКАЗОВ И ДИСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ 200

Богатырев В.А., Паршутина С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МОДЕЛИ МНОГОПУТЕВОЙ ОТКАЗОУСТОЙЧИВОЙ МАРШРУТИЗАЦИИ 201

Богатырев В.А., Паршутина С.А., Попцова Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МНОГОПУТЕВАЯ ОТКАЗОУСТОЙЧИВАЯ МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ И ГИБРИДНЫХ СЕТЯХ С РЕЗЕРВИРОВАННОЙ ПЕРЕДАЧЕЙ ДАННЫХ 202

Богатырев В.А., Сластихин И.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МОДЕЛЬ РЕЗЕРВИРОВАННОГО ОБСЛУЖИВАНИЯ ЗАПРОСОВ В МНОГОКАНАЛЬНЫХ СИСТЕМАХ 202

Бойченко О.В., Адарчина С.О.
Россия, Симферополь, Крымский институт экономики и управления Крымского федерального университета имени В. И. Вернадского
ПРОБЛЕМА ЗАЩИТЫ МАРКЕТИНГОВОЙ ИНФОРМАЦИИ САЙТОВ 203

Васькова А.В., Михайличенко Е.М.
Россия, Санкт-Петербург, Финансовый университет при Правительстве Российской Федерации
ТРАНСПОРТНЫЙ ФАКТОР КАК ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 204

Верзун Н.А., Колбанёв М.О., Михайлов С.В.
Россия, Санкт-Петербург, Международный банковский институт
ТЕХНОЛОГИЧЕСКИЕ ОСНОВАНИЯ ПЕРИОДИЗАЦИИ ИСТОРИИ 205

Верзун Н.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ТЕХНОЛОГИИ БЕЗОПАСНОГО ДОСТУПА В БЕСПРОВОДНЫХ СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ 205

Верзун Н.А., Колбанев А.М., Колбанев М.О
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
Объединенная компания Дом.ru InterZet
АСПЕКТЫ БЕЗОПАСНОСТИ В ДИСЦИПЛИНЕ «ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ» ОБРАЗОВАТЕЛЬНОГО НАПРАВЛЕНИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» 206

Верзун Н.А., Колбанев А.М., Колбанев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
Объединенная компания Дом.ru InterZet
ЭНЕРГЕТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 207

Воробьев А.И. Колбанёв А.М., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Объединенная компания Дом.ru InterZet, Санкт-Петербургский государственный экономический университет
ОПТИМИЗАЦИЯ ИНФРАСТРУКТУРЫ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ 207

Воробьев А.И., Колбанёв А.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Объединенная компания Дом.ru InterZet
ОПТИМИЗАЦИЯ ПРОЦЕССА СЖАТИЯ ДАННЫХ ПО КРИТЕРИЮ ЭНЕРГОПОТРЕБЛЕНИЯ 208

Воробьёв А.И., Колбанёв А.М., Колбанёв М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Объединенная компания Дом.ru InterZet, Санкт-Петербургский государственный экономический университет
АНАЛИЗ ХАРАКТЕРИСТИК ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ С НЕОРДИНАРНЫМ ПОТОКОМ ЗАЯВОК НА ОБСЛУЖИВАНИЕ 208

Воронина Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ УГРОЗ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ 208

Головкин Ю.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
СИТУАЦИОННЫЕ МОДЕЛИ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СИСТЕМАМИ 209

Гусева Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И РИСКИ ПРИ СОВЕРШЕНИИ СТАВОК НА СПОРТИВНЫХ МАТЧАХ 210

Егорова И.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОБ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ 211

Емелин В.И., Колмыков Г.Н.
Россия, Санкт-Петербург, ОАО «НИИ Вектор»
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОЭЛЕКТРОННОГО МОНИТОРИНГА 212

Емельянов А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ 212

Емельянов А.А., Коршунов И.Л.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОПЫТ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ МАЛОГО БИЗНЕСА В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 213

Желваков Б.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
КОРПОРАТИВНЫЕ ЗНАНИЯ В АРХИТЕКТУРЕ СОВРЕМЕННОГО ПРЕДПРИЯТИЯ 214

Иванов В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ОЦЕНКА СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ АСПЕКТОВ БЕЗОПАСНОСТИ СТРАН ЕАЭС 215

Иванов М.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ЭНЕРГОЭФФЕКТИВНОСТЬ ТЕХНОЛОГИЙ КОММУТАЦИИ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 216

Колбанёв А.М.
Россия, Санкт-Петербург, Объединенная компания Дом.ru InterZet
ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 216

Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ФИЗИЧЕСКИЕ РЕСУРСЫ ИНФОРМАЦИОННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ 216

Колбанёв М.О., Коршунов И.Л., Левкин И.М., Микадзе С.Ю.
Россия, Санкт-Петербургский государственный экономический университет
ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА 217

Колбанёв М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ 217

Коломойцев В.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ВОЗМОЖНОСТЕЙ ТИПОВ МЕЖСЕТЕВЫХ ЭКРАНОВ 218

Коршунов И.Л., Пуха Г.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
КОНЦЕПЦИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННОГО ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ФОРМИРОВАНИЯ И РАСПРЕДЕЛЕНИЯ НАГРУЗКИ ВУЗа 219

Левкин И.М., Левкина С.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ИНФОРМАЦИОННАЯ СТРУКТУРА КОНКУРЕНТНОЙ ОБСТАНОВКИ 220

Лобанов В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
АНАЛИЗ РИСКОВ ВЫПОЛНЕНИЯ ПОРТФЕЛЯ ЗАКАЗОВ НА ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ 221

Минаков В.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БАНКОВ 221

Муравьев Е.В., Планкова М.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
АНАЛИЗ ПРИМЕНЕНИЯ SECAAS ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА 222

Николаев М.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ЗАДАЧИ УПРАВЛЕНИЯ ИНФОМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ УСЛОВНОГО ДОСТУПА 223

Омельян А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ СКРЫТОЙ МАРКИРОВКИ ОБЪЕКТОВ ПРИ ПОМОЩИ RFID-МЕТОК 224

Орлов Н.Г.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
БЕЗОПАСНОСТЬ СИСТЕМ МНОЖЕСТВЕННОГО ДОСТУПА ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ 224

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОРГАНИЗАЦИЯ МЕТАДАНЫХ ДЛЯ БЕЗОПАСНОЙ СИСТЕМЫ ДЛИТЕЛЬНОГО ХРАНЕНИЯ..... 224

Пойманова Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
НЕРЕЛЯЦИОННЫЕ БАЗЫ БОЛЬШИХ ДАННЫХ..... 225

Свеженцев И.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
О СОВЕРШЕНСТВОВАНИИ ЗАЩИТЫ ДОСТУПА К ИНФОРМАЦИИ О
ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ..... 225

Соколов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ОЦЕНКА УПРАВЛЕНЧЕСКОЙ ГИБКОСТИ В ПРОЦЕССЕ ПРОЕКТИРОВАНИЯ
ИНФОРМАЦИОННЫХ СИСТЕМ С УЧЕТОМ РИСКА И НЕОПРЕДЕЛЕННОСТИ..... 226

Яковлева М.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
БЕЗОПАСНОСТЬ СИСТЕМЫ УМНЫХ ВЕЩЕЙ 226

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В
КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 227**

Устинов И.А., Виноградов А.А.
Россия, Санкт-Петербург, ОАО «Научно-производственное объединение «Импульс»
НОВЫЕ ВЫЗОВЫ ОТЕЧЕСТВЕННЫМ ТЕХНОЛОГИЯМ АВТОМАТИЗАЦИИ КРИТИЧЕСКИХ
ИНФРАСТРУКТУР..... 227

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля,
судна
ТЕХНОЛОГИИ МИНИМИЗАЦИИ ИЗБЫТОЧНОСТИ ПРИ МОНИТОРИНГЕ И УПРАВЛЕНИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ОБЪЕКТОВ 227

Башкирцев А.С., Паращук И.Б.
Россия, Москва, в/ч 52686,
Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОБОСНОВАНИЕ АКТУАЛЬНОСТИ ФОРМИРОВАНИЯ ПЕРСПЕКТИВНОЙ
ЗАЩИЩЕННОЙАВТОМАТИЗИОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СВЯЗЬЮ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ..... 228

Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
К ВОПРОСУ ЗАЩИТЫ ЗАКРЫТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДНАЗНАЧЕННОГО
НА ЭКСПОРТ..... 229

Жигадло В.Э.
Россия, Санкт-Петербург, ООО «Симпл Групп»
ПРИНЦИПЫ ПОСТРОЕНИЯ И АРХИТЕКТУРА РЕГИОНАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ
«БЕЗОПАСНАЯ ТЕРРИТОРИЯ» 230

Кондратьев Д.А, Ипатов О.С.
Россия, Санкт-Петербург, ОАО «Концерн «Гранит-Электрон»,
Санкт-Петербургский политехнический университет Петра Великого
МЕТОДЫ СИНТЕЗА АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЦЕЛЕУКАЗАНИЯ
И ОСВЕЩЕНИЯ ОБСТАНОВКИ НА БАЗЕ ДИСТАНЦИОННО-ПИЛОТИРУЕМЫХ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ..... 230

Паращук И.Б., Ковальченко Д.А.
Россия, Санкт-Петербург, Военная академия связи имени Маршала Советского Союза С.М. Буденного
ОПРЕДЕЛЕНИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 231

Присяжнюк А.С.
Россия, Санкт-Петербург, ЗАО «Институт телекоммуникаций»
КОГНИТИВНАЯ РАДИОСЕТЬ НА БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТАХ ДЛЯ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ РЕГИОНА 232

Ходаков В.Е., Соколова Н.А., Антипенко И.В., Бабина О.В.
Россия, Керчь, Керченский государственный морской технологический университет
ОЦЕНИВАНИЕ РАЗВИТИЯ ОДНОГО КЛАССА СЛОЖНЫХ СИСТЕМ 232

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГИДРОМЕТЕОРОЛОГИИ 233

Горшков Р.А., Минина М.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОСНОВНЫЕ ПРОБЛЕМЫ СТАНДАРТА БЕЗОПАСНОСТИ BLUETOOTH 233

Игнатьев М.Б.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМЫ ПРОГНОЗИРОВАНИЯ КОСМИЧЕСКОЙ ПОГОДЫ 234

Игнатьев М.Б., Ненашев В.А., Катермина Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Нижневартовск, Нижневартовский государственный университет
ПРОБЛЕМА ПРОГНОЗИРОВАНИЯ ЛИТОСФЕРНОЙ ПОГОДЫ 234

Кочкаров Л.С., Минина М.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ГИДРОГРАФИЯ И ГИДРОМЕТЕОРОЛОГИЯ КАК СОСТАВЛЯЮЩАЯ БЕЗОПАСНОСТИ МОРЕПЛАВАНИЯ 234

Малыгин Е.Ю., Митько В.Б.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОСНОВНЫЕ ПРИЧИНЫ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МОБИЛЬНЫХ УСТРОЙСТВ 234

Митько А.В. , Порокин Д.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОСОБЕННОСТИ СЪЁМКИ РЕЛЬЕФА ДНА ДЛЯ СОЗДАНИЯ МОРСКИХ НАВИГАЦИОННЫХ КАРТВ ИНТЕРЕСАХ БЕЗОПАСНОСТИ МОРЕПЛАВАНИЯ 235

Митько А.В., Синицына А.А.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ГИДРОГРАФИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СУДОХОДСТВА. ГИДРОМЕТЕОРОЛОГИЧЕСКАЯ ПОДДЕРЖКА ИНЖЕНЕРНЫХ ИЗЫСКАНИЙ 235

Митько А.В., Сальцберг Э.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
АНАЛИЗ ПРАВОВЫХ АСПЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ 236

Минина М.В.., Сальцберг Э.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ 236

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ..... 238

Алексеева-Попова Н.В., Дроздова И.В., Калимова И.Б., Беляева А.И.
Россия, Санкт-Петербург, Ботанический институт им. В.Л. Комарова Российской академии наук
ПЕРСПЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ АККУМУЛИРУЮЩИХ СВОЙСТВ РАСТЕНИЙ ДЛЯ СНИЖЕНИЯ РИСКА ЗАГРЯЗНЕНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ ТЯЖЕЛЫМИ МЕТАЛЛАМИ 238

Афанасьев В.П.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ФОРМИРОВАНИЕ И ИССЛЕДОВАНИЕ ВЫСОКОЭФФЕКТИВНЫХ ФОТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ НА ОСНОВЕ ГЕТЕРОСТРУКТУР АМОРФНЫЙ/МОНОКРИСТАЛЛИЧЕСКИЙ КРЕМНИЙ..... 239

Биненко В.И.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук
ИНФОРМАЦИОННАЯ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРИ СОВРЕМЕННОМ ИЗМЕНЕНИИ КЛИМАТА..... 240

Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОМПЛЕКСНЫЙ МОНИТОРИНГ СОСТОЯНИЯ ПРИПРОДНОЙ СРЕДЫ – ОСНОВНОЙ ИСТОЧНИКИНФОРМАЦИИ ОБ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА 240

Васильев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИССЛЕДОВАНИЕ УЛЬТРАФИОЛЕТОВЫХ ФОТОПРИЕМНИКОВ НА ОСНОВЕ КАРБИДА КРЕМНИЯ 241

Величко А.Н., Захаров И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАТИВНЫХ ПАРАМЕТРОВ О ДЕЙСТВИИ ИНГИБИТОРОВ ДЫХАТЕЛЬНОГО ПУТИ НА ТЕРМОТАКСИЧЕСКУЮ РЕАКЦИЮ ПРОСТЕЙШИХ 241

Венедиктов В.Ю., Горелая А.В., Шалымов Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ГРОЗОВЫХ ОБЛАКОВ С ПОМОЩЬЮ ЭФФЕКТА КЕРРА 242

Викторов С.В.
Россия, Санкт-Петербург, Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук,
Санкт-Петербургский государственный университет
СОВРЕМЕННАЯ МОРЕХОЗЯЙСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ В ФИНСКОМ ЗАЛИВЕ СКВОЗЬ ПРИЗМУ ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ 243

Горохов В.Л., Бузников А.А., Федкович О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОГНИТИВНЫЙ МОНИТОРИНГ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ НА ОСНОВЕ МНОГОМЕРНЫХ ДАННЫХ РЕГИОНАЛЬНЫХ СЛУЖБ ЗДРАВООХРАНЕНИЯ 243

Горяинов В.С., Бузников А.А., Черноок В.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), ОАО «Гипрорыбфлот»
АВТОМАТИЗАЦИЯ ОЦЕНКИ ВЕРОЯТНОЙ ИНФОРМАТИВНОСТИ ЛИДАРНОГО ЭХО-СИГНАЛА.... 244

Гульков В.Н., Федоров Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРИМЕНЕНИЕ СИСТЕМЫ ПРОСТРАНСТВЕННОГО ПОЗИЦИОНИРОВАНИЯ СОЛНЕЧНЫХ МОДУЛЕЙ С ЦЕЛЬЮ ПОВЫШЕНИЯ ИХ ЭФФЕКТИВНОСТИ В УСЛОВИЯХ ИЗМЕНЕНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ 244

Доронин А.П., Щукин Г.Г., Дидык О.И., Козлова Н.А., Петроченко В.М., Фролов К.О., Шмалько С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПЕРЕЧЕНЬ ЭКОЛОГИЧЕССКИХ ПРОБЛЕМ, РЕШЕНИЕ КОТОРЫХ ВОЗМОЖНО ПРИ МОДИФИЦИРОВАНИИ ОБЛАКОВ И ТУМАНОВ ЕСТЕСТВЕННОГО И ИСКУССТВЕННОГО ПРОИСХОДЕННИЯ..... 245

Доронин А.П., Дидык О.И., Козлова Н.А., Петроченко В.М., Шмалько С.А., Фролов К.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПЕРЕЧЕНЬ ГЕОФИЗИЧЕСКИХ ПРОЦЕССОВ И ЯВЛЕНИЙ КАК ВОЗМОЖНЫХ ОБЪЕКТОВ МОДИФИЦИРОВАНИЯ В ИНТЕРЕСАХ РЕШЕНИЯ ЭКОЛОГИЧЕСКИХ ПРОБЛЕМ..... 245

Дроздова И.В., Шилин Б.В.
Россия, Санкт-Петербург, Ботанический институт им. В.Л. Комарова Российской академии наук, Центр экологической безопасности Российской академии наук
РАННЯЯ ДИАГНОСТИКА СТРЕССА РАСТИТЕЛЬНОСТИ И ЗАГРЯЗНЕНИЯ ПОЧВЫ ТЯЖЁЛЫМИМЕТАЛЛАМИ ВИДЕОСПЕКТРАЛЬНЫМ МЕТОДОМ 246

Елизаров В.В., Кащеев С.В., Гришканич А.С., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
НОВЫЕ ПОДХОДЫ К РАЗРАБОТКЕ АППАРАТНО-ПРОГРАММНОЙ СИСТЕМЫ УПРАВЛЕНИЯ И РЕГИСТРАЦИИ ЛИДАРНЫХ СИГНАЛОВ В ГИГАГЕРЦОВОМ ДИАПАЗОНЕ ЧАСТОТ 246

Новиков А.В., Тимощук А.С.
Россия, Санкт-Петербург, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРЕДЛОЖЕНИЯ ПО РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА НА БАЗЕ ГИДРОМЕТЕОРОЛОГИЧЕСКОЙ СЛУЖБЫ ВС РФ..... 247

Новиков А.В., Тимощук А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МЕТОДИКА ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ НА ТЕРРИТОРИИ ПРОЕКТИРУЕМОГО ОБЪЕКТА СТРОИТЕЛЬСТВА 248

Парфенов В.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
МЕТОД СПЕКТРОСКОПИИ ЛАЗЕРНОЙ ИСКРЫ И ЕГО ПРИМЕНЕНИЕ ДЛЯ МОНИТОРИНГА ИСТОРИЧЕСКИХ ПАМЯТНИКОВ..... 249

Рузанкина Ю.С., Васильев О.С., Вейко В.П., Гришканич А.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПОВЫШЕНИЕ КОРРОЗИОННОЙ СТОЙКОСТИ ТРУБ НЕФТЕПРОВОДОВ МЕТОДАМИ ФОТОНИКИ 249

Смирнов Л.В., Гришканич А.С., Кащеев С.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
ОАО «НПК «Государственный оптический институт им С.И. Вавилова»
ЛАЗЕРНЫЙ КОМПЛЕКС ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ ОБЪЕКТОВ ТЭК 250

Фурина В.Н., Горохов В.Л., Бузников А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный архитектурно-строительный университет, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
КОМПЬЮТЕРНЫЙ МОНИТОРИНГ И ОЦЕНКА БИОЛОГИЧЕСКОГО РАЗНООБРАЗИЯ И УСТОЙЧИВОСТИ ДРЕВЕСНЫХ РАСТЕНИЙ В УСЛОВИЯХ ГОРОДСКОЙ СРЕДЫ 250

Яковлев А.А., Рузанкина Ю.С., Кащеев С.В., Гришканич А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ ПО УСКОРЕННИЮ РОСТА СЕМЯН С ПОМОЩЬЮ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ 251

Ярошевич Л.И.
Россия, Санкт-Петербург, Санкт-Петербургский государственный институт кино и телевидения
КАРТИННАЯ ПЛОСКОСТЬ ФАСАДА 251

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 253

Алексеев А.В., Ушакова Н.П., Поленин В.И., Соловьев С.Н., Москаленко В.А.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ СУДНА: РЕЗУЛЬТАТЫ ПОДГОТОВКИ КОЛЛЕКТИВНОЙ МОНОГРАФИИ 253

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ТЕХНОЛОГИЯ СИНТЕЗА ФУНКЦИОНАЛЬНЫХ ПОДСИСТЕМ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ СПЕЦИАЛЬНЫХ ОБЪЕКТОВ ВМФ 254

Алексеев С.А., Алексеева Е.К.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ПРИНЦИПЫ СОЗДАНИЯ ОБЩЕГО ИНФОРМАЦИОННОГО РЕСУРСА ВМФ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ 255

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ТЕХНОЛОГИЯ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ СРЕДСТВ И СИСТЕМ ОБЕСПЕЧЕНИЯ ИБ: МАСТЕР-КЛАСС 256

Алексеев А.В., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ТЕХНОЛОГИЯ И ПРОГРАММНЫЙ КОМПЛЕКС МОНИТОРИНГА И УПРАВЛЕНИЯ ЗАЩИЩЕННОСТЬЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ 258

Алексеев А.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
СОВРЕМЕННАЯ ТЕОРИЯ ОПТИМИЗАЦИИ ИНФОРМАЦИОННОЙ ИЗБЫТОЧНОСТИ ДИСКРЕТНОГО ПРЕДСТАВЛЕНИЯ ПРОЦЕССОВ ПРИ МОНИТОРИНГЕ И УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ 259

Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АЛГОРИТМ ОЦЕНКИ АГРЕГИРОВАННОГО ПОКАЗАТЕЛЯ КАЧЕСТВА ОБЕСПЕЧЕНИЯ ИБ 260

Алексеев А.В., Ливанов И.В.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
WEB-РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ СПРУ ДЛЯ РУКОВОДИТЕЛЕЙ ОМТИ 261

Баркова Н.А., Грищенко Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЗАЩИТНОГО МОНИТОРИНГА СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ 262

Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
АНАЛИЗ ОПЫТА ОРГАНИЗАЦИИ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИЯ КАЧЕСТВА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ..... 263

Бучина Д.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
КРИТИЧЕСКИЕ УГРОЗЫ И УЯЗВИМОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ 265

Горбачев Р.И.
Россия, Санкт-Петербург, Институт автоматизации процессов борьбы за живучесть корабля, судна
СРЕДСТВА ЗАЩИТЫ ТЕХНОЛОГИЙ WI-FI И ИХ УЯЗВИМОСТИ..... 265

Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ИНФОРМАЦИОННАЯ МАСКИРОВКА И ДЕЗИНФОРМАЦИЯ ПРИ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ 267

Зайнуллин О.Ф.
Россия, Санкт-Петербург, ОАО «СПМБМ «Малахит»
РЕШЕНИЕ ЗАДАЧ НАДВОДНОЙ НЕПОТОПЛЯЕМОСТИ В СИП БЖ ПОДВОДНЫХ ЛОДОК 268

Кальбфляйш В.А., Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ ПОЛЬЗОВАНИИ СМАРТФОНАМИ И ПЛАНШЕТАМИ 268

Карымов А.В., Митько А.В.
Россия, Санкт-Петербург, Российский государственный гидрометеорологический университет
ОСОБЕННОСТИ АВТОМАТИЧЕСКОЙ ИНДЕНТИФИКАЦИОННОЙ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДОХОДСТВА..... 269

Кузнецов А.Ю., Алексеев А.В.
Россия, Санкт-Петербургский государственный морской технический университет
АВТОМАТИЧЕСКАЯ ДИСТАНЦИОННАЯ МЕДИЦИНСКАЯ ДИАГНОСТИКА И КОНСУЛЬТИРОВАНИЕ В ИНФОРМАЦИОННО ЗАЩИЩЁННОМ ИСПОЛНЕНИИ..... 270

Кузнецов В.В., Согонов С.А., Алексеев А.В., Туркин И.И., Хруцкий О.В., Равин А.А., Шамберов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
НАУЧНЫЕ НАПРАВЛЕНИЯ И НАУЧНЫЕ ШКОЛЫ ОБЕСПЕЧЕНИЯ РАЗВИТИЯ СИСТЕМ АВТОМАТИЗАЦИИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 272

Кузьменко А.В.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ В ИНТЕГРИРОВАННЫХ СИСТЕМАХ ПОДДЕРЖКИ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ 273

Леберянский А.П.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
ВЗАИМОСВЯЗЬ ЗАДАЧ ПО БОРЬБЕ ЗА ЖИВУЧЕСТЬ И ЗАДАЧ ПО ПРЕДУПРЕЖДЕНИЮ АВАРИЙНОСТИ 273

Лобанов С.Л., Бледнов Д.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
ЭВОЛЮЦИЯ ТРЕБОВАНИЙ К АВТОМАТИЗАЦИИ ПРОЦЕССА БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА 276

Малов С.С., Шиманчук С.Н.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕДАЧИ ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ КРЮИНГОВОЙ ОРГАНИЗАЦИИ 277

Мельников А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ 278

Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СИСТЕМА УПРАВЛЕНИЯ ДВИЖЕНИЕМ СУДНА ПО КУРСУ С ПОВЫШЕННОЙ ЖИВУЧЕСТЬЮ 279

Москаленко В.А., Калюта Н.Г.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
МОДЕЛЬ ЖИВУЧЕСТИ КОРАБЛЯ И ЕГО ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ ВНЕШНИХ ПОРАЖАЮЩИХ ВОЗДЕЙСТВИЯХ 280

Пегушин О.В., Аскеров Р.А., Москаленко В.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ РИСКОВ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ РАБОТ ПО ВОССТАНОВЛЕНИЮ ТЕХНИЧЕСКОЙ ГОТОВНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЕЙ ВМФ РФ 281

Пиглюк Р.Н., Шавинская С.К.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
РАЗРАБОТКА МЕТОДА СРАВНЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ЗНАНИЙ 282

Поленин В.И., Можаев А.С., Можаева И.А.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
КОНЦЕПЦИЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ МАКРОУРОВНЕВОГО ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ВЫПОЛНЕНИЕМ ЗАДАЧ С ПРИМЕНЕНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ 283

Равин А.А., Хруцкий О.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ЭВОЛЮЦИЯ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ СУДОВОГО ОБОРУДОВАНИЯ 283

Разживин Н.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ИНФОРМАЦИОННЫЕУЯЗВИМОСТИИ УГРОЗЫ ВОДИТЕЛЯПРИ РЕШЕНИИЗАДАЧ НАВИГАЦИИ .. 285

Рыжиков Ю.И., Алексеев А.В., Лохвицкий В.А.
Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского,
Институт автоматизации процессов борьбы за живучесть корабля, судна
ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ЛУЧЕВЫХ ДИАГРАММ ПРИ ПОЛИМОДЕЛЬНОМ ОЦЕНИВАНИИИ АНАЛИЗЕ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮКРИТИЧЕСКИХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ 286

Савченко Б.В.
Россия, Санкт-Петербург, Санкт-Петербургской государственный морской технический университет
РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АЛГОРИТМЫ ПОИСКА ПУТИ ЗАЩИТЫ И ИХ ОПТИМИЗАЦИЯ 287

Салащенко А.И., Леберянский А.П.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНЫХ ЛОДОК 288

Сергейчик М.В.
Россия, Санкт-Петербург, ОАО «Концерн «НПО «Аврора»
АЛГОРИТМ УПРАВЛЕНИЯ СКОРОСТЬЮ ПЕРЕКЛАДКИ РУЛЕВЫХ УСТРОЙСТВ ОТ СИСТЕМ УПРАВЛЕНИЯ ДВИЖЕНИЕМ И ЕГО ИНФОРМАЦИОННАЯ ЗАЩИЩЕННОСТЬ 289

Сухов Р.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СИСТЕМА ВИЗУАЛЬНОГО УПРАВЛЕНИЯ АВТОМАТИЗИРОВАННЫМИ УСТРОЙСТВАМИ 290

Тарабаров А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВ АВТОРИЗАЦИИ И ВОЗМОЖНОСТЕЙ ИХ СОВЕРШЕНСТВОВАНИЯ 291

Тобольченко А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРИ РЕШЕНИИ ЗАДАЧИ О НОРМИРОВАНИИ ИТОГОВЫХ ПОКАЗАТЕЛЕЙ СИСТЕМ УПРАВЛЕНИЯ СО СТАТИСТИЧЕСКОЙ НЕПОЛНОТОЙ 292

Тобольченко А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
МАТЕМАТИЧЕСКИЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ СО СТАТИСТИЧЕСКОЙ НЕПОЛНОТОЙ 293

Тобольченко А.С., Жуланова Д.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ИСПОЛЬЗОВАНИЕ ПОДХОДА ГРУППОВОГО (ВЕСОВОГО) КОНТРОЛЯ ПРИ ОРГАНИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ МЕТОДАМИ ИНФОРМАЦИОННОЙ МАСКИРОВКИ И ДЕЗИНФОРМАЦИИ 294

Туркин И.И.,Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ОСОБЕННОСТИ АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЖИВУЧЕСТИ СУДОВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ 295

Туркин И.И., Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
УПРАВЛЕНИЕ ДВИЖЕНИЕМ СУДНА ПО КУРСУ С ПОВЫШЕННОЙ ЖИВУЧЕСТЬЮ 296

Туркин И.И.,Алексеев А.В., Мин Хеин
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
К ВОПРОСУ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ АВТОМАТИЗИРОВАННЫХ СУДОВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ 297

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНИЧЕСКИХ СРЕДСТВ МАССОВОГО СПРОСА..... 298

Тюрин И.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРОГРАММНЫЙ КОМПЛЕКС ОБЪЕКТИВНОЙ ОЦЕНКИ КАЧЕСТВА РАЗНОРОДНЫХ ОБЪЕКТОВВ ЗАЩИЩЕННОМ ИСПОЛНЕНИИ 299

Шаров А.И. , Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ ТЕЛЕФОНОВ 300

Шитикова К.А.. Тюрин И.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ ИСПОЛЬЗОВАНИИ ОФИСНОЙ ТЕХНИКИ 301

Удодова Е.Н.
Россия, Санкт-Петербург, ФГУП «Крыловский государственный научный центр»
МЕТОДИКА АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ И МОНИТОРИНГА КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЙ СУДОСТРОИТЕЛЬНОЙ ПРОМЫШЛЕННОСТИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ..... 302

Урубков П.И., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
ПРАКТИКА ИНФОРМАЦИОННО-ПОИСКОВОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ «АНТИПЛАГИАТ».. 303

Ушакова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
АНАЛИЗ ТЕХНОЛОГИЙ И ВОЗМОЖНОСТЕЙ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ В СУДОВЫХ СИСТЕМАХ СВЯЗИ 304

Ушакова Н.П., Москаленко В.А.
Россия, Санкт-Петербург, ОАО «Концерн «НПО «Аврора», Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
СОЗДАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ БОРЬБЕ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ..... 305

Филиппова А.С., Алексеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный морской технический университет
СЕТЕВОЙ МОНИТОРИНГ БЕЗОПАСНОСТИ МОРСКИХ ОБЪЕКТОВ 306

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ..... 308

Долженкова Е.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
РОЛЬ НОВЫХ ЧЛЕНОВ ЕВРОПЕЙСКОГО СОЮЗА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА НАТО 308

Забарин А.В., Зимичев А.М., Мезенцев Д.Ф.
Россия, Санкт-Петербург, Санкт-Петербургский военный институт внутренних войск МВД России, Санкт-Петербургский государственный университет
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА 309

Карпович С.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ТЕМАТИЧЕСКОЙ МОДЕЛИ С НЕПРЕРЫВНЫМ ВРЕМЕНЕМ ДЛЯ КОНТРОЛЯ ПУБЛИКАЦИЙ В СЕТИ ИНТЕРНЕТ 309

Кефели И.Ф.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
«ШЕСТОЕ ИЗМЕРЕНИЕ» ГЛОБАЛЬНОЙ ВОЙНЫ И ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ 310

Кефели И.Ф., Меркулов А.Л.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ГЛАВНАЯ ПРИЧИНА РАСПАДА СССР 312

Киряхин Н.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 312

Колотов В.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
А. ДАЛЛЕС О МЕТОДАХ ВЕДЕНИЯ ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ И СОВРЕМЕННОЕ СОСТОЯНИЕ БИТВЫ «ЗА УМЫ И СЕРДЦА» 313

Комлева Н.А.
Россия, Екатеринбург, Центр геополитического анализа
ИДЕОЛОГИЧЕСКАЯ ГРАНИЦА КАК ПРЕДЕЛ БЕЗОПАСНОСТИ ИДЕОЛОГИЧЕСКОГО ПРОСТРАНСТВА 314

Левкин И.М., Левкин Е.О.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОДИКА ВЫЧИСЛЕНИЯ ИНДЕКСА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ 315

Леонов А.В., Колмаков С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОГРАММИСТА ПРИ РАБОТЕ С СОВРЕМЕННЫМИ ИНТЕГРИРОВАННЫМИ СРЕДАМИ РАЗРАБОТКИ (IDE) 315

Москвин С.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
СИСТЕМА ИНФОРМАЦИОННЫХ ПАРАДОКСОВ И ЕЕ ПРИМЕНЕНИЕ В ПАРИРОВАНИИ УГРОЗ ГИБРИДНОЙ ХОЛОДНОЙ ВОЙНЫ 316

Нурышев Г.Н.
Россия, Санкт-Петербург, Санкт-Петербургский государственный экономический университет
ИНФОРМАЦИОННАЯ ГЕОПОЛИТИКА: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ 316

Пилькевич С.В., Еремеев М.А., Мажников П.В.
Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского
МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ГРУПП ПОЛЬЗОВАТЕЛЕЙ СОВРЕМЕННЫХ СРЕДСТВ МАССОВОЙ КОММУНИКАЦИИ В РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ 317

Плебанек О.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ 318

Попов П.В.
Россия, Санкт-Петербург, Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ПОЛИТИЧЕСКИЕ ФАКТОРЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ 320

Пронин А.С.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПРОПАГАНДИСТСКАЯ ДЕЯТЕЛЬНОСТЬ ЭКСТРЕМИСТСКИХ ОРГАНИЗАЦИЙ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА 321

Свешникова Н.О.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет
ПСИХОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ 322

Худяков А.И., Худякова Е.А.
Россия, Санкт-Петербург, Российский государственный педагогический университет им. А.И. Герцена
ПСИХИКА. ИНФОРМАЦИЯ. БЕЗОПАСНОСТЬ 323

Шацкая В.И.
Россия, Санкт-Петербург, Северо-Западное отделение Академии геополитических проблем
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА НАСЕЛЕНИЕ (НА ПРИМЕРЕ УКРАИНСКОГО КРИЗИСА И РАЗВЕРТЫВАНИЯ ГЛОБАЛЬНОЙ СИСТЕМЫ ПРО США) 323

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ 325

Абиссова М.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ И СЕРВИСЫ ОБУЧЕНИЯ ДИСЦИПЛИНЕ «МИРОВЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ» В ВЫСШЕЙ ШКОЛЕ 325

Абрамов М.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
КОМПЛЕКС ПРОГРАММ ДЛЯ АНАЛИЗА ДОСТИЖИМОСТИ КРИТИЧНЫХ ДОКУМЕНТОВ И ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ 326

Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
КОМПЛЕКС «КРИТИЧЕСКИЕ ДОКУМЕНТЫ — ИНФОРМАЦИОННАЯ СИСТЕМА — ПЕРСОНАЛ — ЗЛОУМЫШЛЕННИК» 326

Азаров А.А.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
АЛГОРИТМЫ РАСЧЕТА ВЕРОЯТНОСТНЫХ ОЦЕНОК ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА НА ОСНОВЕ МАРКОВСКИХ СЕТЕЙ..... 327

Баев В.А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ХРОНОТИПА ПОЛЬЗОВАТЕЛЯ ПО ЕГО ЦИФРОВЫМ СЛЕДАМ..... 327

Блюм В.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
МАСТЕР-ИНДЕКС ПАЦИЕНТОВ ДЛЯ МОДЕЛИ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ И ЕГО ИНФОРМАЦИОННАЯ УСТОЙЧИВОСТЬ 327

Блюм В.С., Заболотский В.П.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ВЕКТОРНО-СОБЫТИЙНАЯ МОДЕЛЬ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ И ЕЁ СОЦИАЛЬНОЕ ЗНАЧЕНИЕ..... 328

Валькова Т.В., Суровенко И.А., Влащенко А.О,
Россия, Санкт-Петербург, 9 отдел БСТМ ГУ МВД России по СПб и ЛО,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГРАЖДАНИНА. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ «САМОГО СЕБЯ» 328

Верещагин В.Л., Муллина Э.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТЯХ, ПОСТРОЕННЫХ НА КОММУТАТОРАХ CISCO..... 329

Гейгер Г., Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ СИСТЕМ ЗАЩИТЫ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯБЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОБЪЕКТАХ..... 330

Левко Г.М, Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
АВТОРСКИЕ ПРАВА И ИХ ЗАЩИТА В СИСТЕМЕ ИНТЕРНЕТ 330

Самборский И.М., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ВЫЯВЛЕНИЕ АККАУНТОВ, НЕ ПРЕДСТАВЛЯЮЩИХ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ..... 331

Святкина М.Н.
Россия, Москва, Московский государственный технический университет им. Н.Э. Баумана
ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ КОГНИТИВНОЙ ГРАФИКИ В СИСТЕМАХ МОНИТОРИНГА СЛОЖНЫХ ТЕХНИЧЕСКИХ ОБЪЕКТОВ..... 331

Семенов А., Фильченков А.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Москва, Московский государственный гуманитарный университет им. М.А. Шолохова
ВЫЯВЛЕНИЕ ДЕМОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ВЫЯВЛЕНИЯ МУЗЫКАЛЬНЫХ ПРЕДПОЧТЕНИЙ 332

Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
ТЕСТИРОВАНИЕ ИНСТРУМЕНТАРИЯ ДЛЯ ОЦЕНИВАНИЯ ИНТЕНСИВНОСТИ УГРОЗООБРАЗУЮЩЕГО ПОВЕДЕНИЯ РЕСПОНДЕНТОВ 332

Тишкина Н.В., Хабарова Г.В.
Россия, Санкт-Петербург, Санкт-Петербургский университет МВД России
СЕТЬ ИНТЕРНЕТ И ЗАШИТА ИНФОРМАЦИИ..... 332

Торопова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СОЗДАНИЕ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ДИАГНОСТИКИ СОГЛАСОВАННОСТИ ДАННЫХ В МОДЕЛИ ОЦЕНКИ ИНТЕНСИВНОСТИ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ 333

Тулупьев А.Л.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербургский государственный университет
ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ В ЗАДАЧАХ СОЦИАЛЬНОГО КОМПЬЮТИНГА, СВЯЗАННЫХ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ 334

Тулупьева Т.В., Тафинцева А.С.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Северо-Западный институт управления РАНХиГС
СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК СВЕДЕНИЙ ДЛЯ ПОСТРОЕНИЯ ПСИХОЛОГИЧЕСКОГО ПОРТРЕТА 334

Тулупьева Т.В., Суворова А.В.
Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации Российской академии наук
СИСТЕМА КЛАССИФИКАЦИИ ПОСТОВ КАК ЭТАП ДИАГНОСТИКИ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ 335

Федотова А.В., Бурдо Г.Б.
Россия, Москва, Московский государственный технический университет им. Н.Э.Баумана
Тверь, Тверской государственный технический университет
РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ АСУТП ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ..... 335

Федотова А.В., Давыденко И.Т., Святкина М.Н., Шункевич Д.В.
Россия, Москва, Московский государственный технический университет им. Н.Э.Баумана,
Республика Беларусь, Минск, Белорусский государственный университет информатики и радиоэлектроники
ОНТОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДЛЯ РЕАЛИЗАЦИИ СЕМАНТИЧЕСКИХ ТЕХНОЛОГИ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ 336

Федотова А.В., Ярушев С.А.
Россия, Москва, Московский государственный технический университет им. Н.Э.Баумана,
Международный университет природы, общества и человека «Дубна»
ГИБРИДНЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ 336

Федотова А.В., Табаков В.В.
Россия, Москва, Московский государственный технический университет им. Н.Э. Баумана,Институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук
БОЛЬШИЕ ДАННЫЕ КАК ИНСТРУМЕНТ ПРЕОДОЛЕНИЯ ИНФОРМАЦИОННОГО БАРЬЕРА В СОЦИОКОМПЬЮТИНГЕ..... 337

Флеров В.Д., Эм П.С.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
СОЗДАНИЕ ЕДИНОЙ СИСТЕМЫ ДОСТУПА К СЕТИ ИНТЕРНЕТ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ 337

Фокин Р.Р.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОЙ МОБИЛЬНОСТИ 338

Эм П.С., Флеров В.Д.
Россия, Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова
МЕТОДЫ БОРЬБЫ С ПОЛУЧАЕМОЙ В ИНТЕРНЕТЕ ЗАПРЕЩЁННОЙ ИНФОРМАЦИЕЙ С ПОМОЩЬЮ АНОНИМАЙЗЕРОВ 339

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 341

Балыкбаева У.А., Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ПРИНЦИПЫ СООТНОШЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ И ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ 341

Барабаш П.А.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ОСОБЕННОСТИ ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ» 341

Башун В.В., Сергеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ЛИЧНЫЙ ЭЛЕКТРОННЫЙ КАБИНЕТ ПРЕПОДАВАТЕЛЯ КАК ВАЖНЫЙ ЭЛЕМЕНТ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ ПРОЗРАЧНОСТИ СОВРЕМЕННОГО ВУЗА 342

Бучкова Е.С., Быстрова О.Д., Федоров Д.Ю., Солодянников А.В.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ПЕРСПЕКТИВЫ РАЗРАБОТКИ И АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ 343

Верещагин В.Л.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
РОЛЬ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСПЕКТЕ ЗАДАЧИ УЛУЧШЕНИЯ РОССИЙСКОЙ СИСТЕМЫ ОБРАЗОВАНИЯ 344

Гаврилов Л.С.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ИНТЕРФЕЙС ДЛЯ МОБИЛЬНОЙ ВЕРСИИ ГРАФИЧЕСКОГО ПРИЛОЖЕНИЯ KRITA SKETCH 345

Гейгер Г.В., Муллина Э.В., Радченко Н.В., Самойленко Е.А.
Россия, Санкт-Петербург, ЗАО «Ассоциация специалистов информационных систем»
ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ВЗГЛЯД ДИПЛОМИРОВАННЫХ СПЕЦИАЛИСТОВ: АКТУАЛЬНОСТЬ, ПРАКТИЧНОСТЬ, ПЕРСПЕКТИВЫ 345

Захаров К.С., Яковлев С.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ПРИМЕНЕНИЕ КОМПЬТЕРНОГО ОБУЧЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 346

Коваленко Д.И.
Россия, Санкт-Петербург, Научно-исследовательский институт (оперативно-стратегических исследований строительства ВМФ) ВУНЦ ВМФ «Военно-морская академия»
ОСОБЕННОСТИ НЕПРЕРЫВНОЙ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ОФИЦЕРСКОГО СОСТАВА ЭМС В СИСТЕМЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ 347

Лапин В.Н.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «FITNESS-КОНСУЛЬТАНТ» 348

Подружкина Т.А., Федоров Д.Ю.
Россия, Санкт-Петербург, Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербургский государственный экономический университет
ПРОБЛЕМНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СТАНДАРТИЗАЦИИ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ... 349

Пригода А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
БИБЛИОТЕКА ПРОГРАММНЫХ ГРАФИЧЕСКИХ МОДУЛЕЙ ДЛЯ РАЗРАБОТКИ САЙТОВ МАЛЫХ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ 350

Рожкова В.Е.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ АВТОМАТИЗАЦИИ РАБОТ ДЕКАНАТОВ И КАФЕДР ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ 351

Сергеев А.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
УЧЕБНЫЙ КУРС ПО РАЗРАБОТКЕ ВСТРАИВАЕМЫХ СИСТЕМ НА БАЗЕ МИКРО-ПЛАТФОРМ INTEL 351

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
ПОДГОТОВКА КАДРОВ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В РАМКАХ ФЕДЕРАЛЬНЫХ ГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТОВ ЧЕТВЕРТОГО ПОКОЛЕНИЯ 352

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
АКТУАЛИЗАЦИЯ ФГОС ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В РАМКАХ ПРОФИЛЯ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ» 353

Советов Б.Я., Цехановский В.В.
Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РАМКАХ ПОДГОТОВКИ БАКАЛАВРОВ И МАГИСТРОВ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» 354

Усольцев А.В.
Россия, Санкт-Петербург, Смольный институт Российской академии образования
БИБЛИОТЕКА ПРОГРАММНЫХ МОДУЛЕЙ РАСШИРЕНИЯ ФУНКЦИЙ CMS 1С-БИТРИКС И МЕТОДИКА РАЗРАБОТКИ САЙТОВ МАЛЫХ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ 354

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» 356

Абакумов А.А. , Сорокин И.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
УЛУЧШЕНИЕ МЕТОДА РАСПОЗНАВАНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНЫХ ДОМЕННЫХ ИМЕН В СЕТИ ИНТЕРНЕТ..... 356

Белов Н. И., Дубинич Е. А., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ В ЦЕЛЯХ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕНСОРНЫХ СЕТЯХ..... 356

Белов С. В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОПРЕДЕЛЕНИЕ ЭМОЦИОНАЛЬНОГО ОКРАСА ОБЩЕНИЯ ПОЛЬЗОВАТЕЛЯ С СОБЕСЕДНИКАМИ В МЕССЕНДЖЕРАХ 357

Бессонова Е.Е., Демяшев А.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
СОЗДАНИЕ РЕКОМЕНДАЦИЙ К АВТОМАТИЗИРОВАННЫМ СИСТЕМАМ УПРАВЛЕНИЯ (АСУ) «УМНЫХ ДОМОВ» (УД)..... 358

Бессонова Е.Е., Настека А.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ПРОТОКОЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ ДЛЯ РЕАЛИЗАЦИИ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ПРИМЕРЕ СИСТЕМЫ «УМНЫЙ ДОМ» 359

Викснин И.И., Юрьева Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИМИТАЦИОННАЯ МОДЕЛЬ ДЛЯ ОПТИМИЗАЦИИ ПОКАЗАТЕЛЯ ДОСТУПНОСТИ ИНФОРМАЦИИВ МОБИЛЬНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ..... 359

Григорьева Д.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МЕТОД АНАЛИЗА ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАНАЛОВ БЕСПРОВОДНЫХ СЕТЕЙ..... 360

Гусев Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИВАТНОСТЬ В ИНТЕРНЕТЕ 360

Ефремов А.А., Бессонова Е.Е., Канев А.Н., Никифорова К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
МОДЕЛИРОВАНИЕ СИСТЕМЫ, ПОСТРОЕННОЙ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ» КАК ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ 361

Зайцева Н.М.
Россия, Санкт-Петербург, Санкт-петербургский национальный исследовательский университет информационных технологий, механики и оптики
ПРИМЕНЕНИЕ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ ДЛЯ ПЛАНИРОВАНИЯ ЗАТРАТ НА СИСТЕМУ БЕЗОПАСНОСТИ..... 361

Золотарева Е.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
СИСТЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ КАК СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 362

Золотарева К.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ОРГАНИЗАЦИОННЫХ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ЛАЗЕРНЫМ МИКРОФОНАМ 363

Игнатьев М.Б., Бариков Л.Н., Литовкин А.А.
Россия, Санкт-Петербург, Санкт-Петербургский государственный университет аэрокосмического приборостроения
ПРОБЛЕМА БОРЬБЫ С АСТЕРОИДНОЙ ОПАСНОСТЬЮ И КОСМИЧЕСКИМ МУСОРОМ 364

Иванова Т.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
ВЫБОР ПАРАМЕТРОВ КЛАСТЕРИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБНАРУЖЕНИЯ АТАК 364

Ильин А.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
РАЗРАБОТКА СИСТЕМЫ ПРОГРАММНО-АППАРАТНОГО ШИФРОВАНИЯ КАНАЛА СВЯЗИ НА БАЗЕ МИКРОКОНТРОЛЛЕРОВ ФМК 365

Ильин И.В., Бессонова Е.Е.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
«УМНЫЙ ДОМ» КАК МУЛЬТИАГЕНТНАЯ СИСТЕМА ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ 365

Иоффе М.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ВОЗМОЖНОСТЕЙ ЛАЗЕРНОГО МИКРОФОНА И РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕР ПРОТИВОДЕЙСТВИЯ 366

Канев А.Н., Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТРИК 367

Карбутов Е.Д.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ВСЕ ЕЩЕ ЖИВОЙ NTLM 367

Келесис Н.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
СОЗДАНИЕ СПРАВОЧНОГО ПОСОБИЯ, ПОВЫШАЮЩЕГО УРОВЕНЬ ИБ, НА ОСНОВЕ ИССЛЕДОВАНИЯ ВЕКТОРОВ АТАК НА СУБД MSSQL SERVER 368

Кудрявцева К.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ВОЛОКОННО-ОПТИЧЕСКОГО КАНАЛА СВЯЗИ ОТ УГРОЗЫ ПЕРЕХВАТА ТРАФИКА 369

Кузьмич Е.В.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
СТАНДАРТЫ СПЕЦИФИКАЦИИ МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ 370

Лямзина А.Г., Коржук В.М.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ И ОСНОВНЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ПРОГРАММЫ «УМНЫЙ ГОРОД КРОНШТАДТ» 371

Насретдинова Д.Р.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
УНИЧТОЖЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ 371

Нурдинов Р.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ДЕСТРУКТИВНЫХ СОСТОЯНИЙ И ПЕРЕХОДОВ 372

Петрук Т.Н.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИЗГИБ ОПТИЧЕСКОГО ВОЛОКНА КАК ОДИН ИЗ СПОСОБОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ 373

Ральникова Н.С.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОПТИЧЕСКОЕ ТУННЕЛИРОВАНИЕ КАК МЕТОД ФОРМИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ 373

Цымжитов Г.Б.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ОТКРЫТЫЕ ДАННЫЕ. ЭФФЕКТИВНОСТЬ И РЕЗУЛЬТАТИВНОСТЬ МЕР ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ 374

Чалыкин И.Г.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ СУБД «ORACLE» 375

Шевченко Д.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
ВОССТАНОВЛЕНИЕ ИЗОБРАЖЕНИЙ МЕТОДОМ СЛЕПОЙ ДЕКОНВОЛЮЦИИ 375

Шоломов И.А.
Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
АКТУАЛЬНОСТЬ ИННОВАЦИОННОГО ПОДХОДА К АНАЛИЗУ СОСТОЯНИЙ ИБ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ, НА ОСНОВЕ КОМПЛЕКСИРОВАНИЯ ИНФОРМАЦИИ, ПОСТУПАЮЩЕЙ ОТ РАЗНОРОДНЫХ СЕНСОРОВ 376

ОГЛАВЛЕНИЕ 378