САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 1

Санкт-Петербург
2015

http://spoisu.ru

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 1

Санкт-Петербург
2015

http://spoisu.ru

УДК (002:681):338.98

Р32

Р32 **Региональная информатика и информационная безопасность.** Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015. – 572 с.
ISBN 978-5-906782-89-2

Сборник статей охватывает широкий круг направлений Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» и Санкт-Петербургской международной конференции «Региональная информатика», проведенных при поддержке Правительства Санкт-Петербурге в 2013-2015 г.г.: Государственная политика и правовое обеспечение информатизации и информационной безопасности; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Безопасность информационных технологий и средства защиты информации; Информационно-психологическая безопасность; Информационные технологии в экономике и бизнесе; Информационные технологии в критических инфраструктурах; Подготовка и переподготовка ИТ-специалистов. Информационные технологии в образовании; Информационные технологии в здравоохранении; Информационные технологии в управлении; Информационные технологии в экологии; Информационные технологии в социокомпьютинге; Информационные технологии управления объектами морской техники и морской инфраструктуры.

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 информатизации, связи, информационной безопасности и защиты информации.

УДК (002:681):338.98

Ответственные редакторы:
Б.Я. Советов, Р.М. Юсупов, В.П. Заболотский, В.В. Касаткин
Компьютерная верстка: *А.С. Михайлова*

Публикуется в авторской редакции

Подписано в печать 14.10.2015. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 35,8. Тираж 500 экз. Заказ № 1102
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-906782-89-2

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

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 1

St. Petersburg
2015

http://spoisu.ru

http://spoisu.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОТРУДНИЧЕСТВО РОССИЙСКИХ И БЕЛОРУССКИХ УЧЕНЫХ В РАЗРАБОТКЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МПА СНГ

Бачило Иллария Лаврентьевна[1], Вус Михаил Александрович[2], Макаров Олег Сергеевич[3], Юсупов Рафаэль Мидхатович[2]
[1]Институт государства и права Российской академии наук,
Россия, Москва, ул. Знаменка, 10,
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия, 39,
ГУО «Институт национальной безопасности Республики Беларусь»,
Беларусь, Минск, улица Змитрока Бядули 2,
e-mails: illaria1@mail.ru. mixail-vus@ mail.ru, makarovos@list.ru, spiiran@iias.spb.su

Аннотация. В статье освещается сотрудничество российских и белорусских учёных в исследовании вопросов прикладной информатики, информационного права и информационной безопасности, осуществляющееся в рамках разработки проектов, предусмотренных планами законотворческих работ Межпарламентской Ассамблеи Содружества Независимых Государств (МПА СНГ). Описываются результаты совместных разработок интернационального научного коллектива, сформировавшегося из представителей академических институтов Российской Федерации и специалистов государственных образовательных учреждений Республики Беларусь. Акцентировано внимание на актуальности упорядочения понятийного аппарата модельного законодательства. Освещаются вопросы гармонизации национального и модельного законодательства в области обеспечения информационной безопасности на примере новых модельных законов «Об информации, информатизации и обеспечении информационной безопасности» и «О критически важных объектах информационно-коммуникационной инфраструктуры». Одним из актуальных направлений сотрудничества в текущий период является также сравнительное исследование вопросов правового регулирования защиты государственных секретов в государствах СНГ. Опыт сотрудничества дал положительные результаты; наработанные на протяжении ряда лет. Материалы и полученные результаты позволили выйти на разработку проекта документа «Стратегия информационной безопасности для государств – участников СНГ», который успешно прошёл экспертизу в парламентах государств – участников и был принят на 41-й сессии МПА СНГ. Вышел в свет ряд подготовленных справочных словарных изданий. Метод – комплексный подход к теме использования ИКТ в условиях обострения угроз в информационной сфере, сравнительно-правовой анализ. Результат – понятия «информационная безопасность», «правовое обеспечение информационной безопасности», Стратегия обеспечения информационной безопасности, рекомендации для национального законодательства по теме.

Ключевые слова. *Межпарламентская Ассамблея СНГ, информатизация, коммуникации, информационная инфраструктура, критически важные объекты, стратегия безопасности, государственные секреты, информационная безопасность, рекомендации, понятийный аппарат, модельный закон.*

COOPERATION BETWEEN RUSSIAN AND BELARUSIAN SCIENTISTS DEVELOP MODEL LEGISLATION IN THE FIELD OF INFORMATION SECURITY FOR CIS INTERPARLIAMENTARY

Bachilo I.L.[1], Vus M.A.[2], Makarov O.S.[3], Yusupov R.M.[2],
[2]St.Petersburg Institute for Informatics and Automation of the RAS,
[2]Russia, St. Petersburg 14 line, 39,
e-mails: illaria1@mail.ru. mixail-vus@ mail.ru, makarovos@list.ru, spiiran@iias.spb.su

Abstract: The article highlights the cooperation between Russian and Belarusian scientists in the study of issues of applied informatics, information law and information security, carried out within the development projects envisaged in the plan of legislative work of the Interparliamentary Assembly of the Commonwealth Independent States (IPA CIS). It describes the results of joint development of the international research team, consisting of representatives of the academic institutes of the Russian Federation and specialists of

state educational institutions of the Republic of Belarus. The attention is focused on the relevance of the conceptual apparatus of ordering model legislation. Highlights issues of harmonization of national and model laws on information security on the example of the new model laws "On information, informatization and information security" and "On critical facilities information and communication infrastructure." One of the current areas of cooperation in the current period is also a comparative study of the legal regulation of the protection of state secrets in the CIS countries. Experience of cooperation has yielded positive results; tried and tested over the years and the results obtained materials allowed to enter the drafting of the document "Strategy of information security for the states - participants of the CIS", which successfully passed the examination in the parliaments of states - participants and was adopted at the 41st session of the CIS Interparliamentary Assembly. It was published a number of publications produced by reference dictionary. Method – The author used a comprehensive approach to the subject of the ICT using under escalation of information treats and comparative legal analysis. Result – The author defines the concepts of "information security", "legal information security" and offers the information security strategy and recommendations for national legislation on the subject.

Keywords. The Interparliamentary Assembly*, The Commonwealth of Independent States (IPA CIS), information, communications, information infrastructure, critical facilities, security strategy, state secrets, information security, the recommendations, the conceptual apparatus, the model law.*

Введение. Межпарламентская Ассамблея Содружества Независимых Государств (МПА СНГ), функционирующая без малого уже четверть века, состоит из парламентских делегаций государств – участников СНГ. Центральное место в её работе занимают вопросы развития модельного законодательства в интересах государств–участников Содружества. Адаптируя международный опыт применительно к условиям государств–участников, МПА СНГ разрабатывает для них типовые модельные законодательные акты и рекомендации. Эти документы не обладают обязательной юридической силой, однако наличие типовых моделей правового регулирования определённых отношений составляет потенциал для развития национальных систем законодательства в общем ключе. Благодаря их наличию создаётся механизм имплементации положений международно-правовых документов в национальные правовые системы государств – участников СНГ [3, с. 45–55].

Над проектами модельных законов и рекомендаций для МПА СНГ в рамках парламентских комиссий работают парламентарии и эксперты. Только за последнее пятилетие учёными российских академических институтов: Санкт-Петербургского института информатики и автоматизации (СПИИРАН) и Института государства и права (ИГП РАН), в сотрудничестве со специалистами Государственных учреждений образования Республики Беларусь: Институт национальной безопасности, Академия МВД и Институт погранслужбы, выполнен ряд интеграционных разработок и подготовлены проекты десятка международных документов, относящихся к области информатизации, информационного права и информационной безопасности [1, с. 8–11].

Разработки концептуального характера

Концепцией сотрудничества государств – участников СНГ в области обеспечения информационной безопасности, принятой Советом глав государств СНГ в 2008 году, предусматривалась разработка рекомендаций по совершенствованию и гармонизации национального законодательства в сфере обеспечения информационной безопасности. В планах модельного законотворчества, в силу ряда причин, этот вопрос нашел своё отражение с некоторым запозданием. В итоге попытку подготовки проекта такого документа предпринял инициативно сформированный СПИИРАН интернациональный коллектив российских и белорусских учёных. Целью этой разработки явилось формулирование общих подходов для государств – участников СНГ к правовому регулированию в данной предметной области [2, с. 24–27].

Разработчики документа «Рекомендации по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности» предложили опереться на трактовку понятия «информационная безопасность», использованную в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности государств – членов Шанхайской организации сотрудничества (2009 г.). При этом было обращено внимание на актуальность и необходимость обеспечения терминологической ясности и единообразного понимания (трактовок) законодательными органами государств – участников СНГ широкоупотребительных сегодня понятий, включая базовые общетехнические категории информационной сферы [4, с. 22–27; 5, с. 7–15].

Проект разрабатывавшегося для МПА СНГ, концептуального по своему характеру документа, в 2010–2012 гг. публиковался для широкого обсуждения на страницах ряда периодических научных изданий, что в конечном итоге предопределило успешное завершение работы над ним. Прошедшие экспертизу в парламентах государств – участников Содружества «Рекомендации по совершенствованию и гармонизации национального законодательства в сфере информационной безопасности» были приняты на 38-м пленарном заседании МПА СНГ в 2012 г. [6, с. 161–179]. В том же году вышел в свет подготовленный авторским коллективом словарь понятийного аппарата

модельного законодательства, годом позже отмеченный профессиональной премией Национального ИНФОФОРУМА по информационной безопасности [7].

Интенсивное развитие инфраструктур в различных сферах жизнедеятельности государства и возрастание сложности, в том числе информационно-коммуникационной инфраструктуры, обуславливает увеличение числа различного рода критически важных объектов, нарушение нормального функционирования или выведение из строя которых может привести к тяжким (а в ряде случаев — необратимым) последствиям, для страны, региона и, как следствие, населения. Наличие в любом государстве критически важных объектов информатизации обуславливает необходимость разработки специальных регламентов административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности. Предметом правового регулирования в рамках таких регламентов должны быть правовые и организационно-управленческие отношения, связанные с формированием механизма реализации полномочий государственных органов, а также прав и законных интересов заинтересованных субъектов в сфере эксплуатации критически важных объектов [8, с. 27–29].

Расширяющиеся возможности глобальных компьютерных информационных и телекоммуникационных сетей обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций. Борьба с терроризмом относится сегодня к приоритетным задачам обеспечения безопасности, и задачи правового регулирования предупреждения использования информационных сетей в террористических и иных противоправных целях исключительно актуальны для всех стран Содружества. Актуальность этого нисколько не снижает существующий сегодня между различными государствами определённый разрыв в развитии телекоммуникаций и в продвижении к информационному обществу.

В рамках мероприятий Программы сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма в 2013 г. инициативно сформировавшимся вокруг СПИИРАН российско-белорусским коллективом учёных была завершена работа по разработке проекта: «Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях». В качестве принципов совершенствования правового регулирования эксплуатации открытых телекоммуникационных сетей (ОТКС) в этих Рекомендациях были выделены: рациональное разграничение компетенции государственных органов различного уровня и иных организаций, действующих в рассматриваемой области; совершенствование их координации и взаимодействия; криминализация общественно опасных деяний (преступлений), связанных с использованием ОТКС в террористических и иных противоправных целях, а также установление адекватных мер административной и дисциплинарной ответственности за административные правонарушения и дисциплинарные проступки; обеспечение неотвратимости наказания [9, с. 23–25]. Такой подход получил одобрение, а разработанный документ, успешно прошедший экспертизу в парламентах государств – участников, был принят МПА СНГ в 2013 г. [10, с. 458–477].

В 2014 г. тем же российско-белорусским научным коллективом были разработаны проекты: «Стратегия обеспечения информационной безопасности государств – участников СНГ»; «Модельный регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ» и Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры». В ходе выполнения работы по этой программе было предусмотрено внести изменения в Модельный закон «Об информатизации, информации и защите информации» (2005 г.). Эта часть задания завершилась разработкой и принятием нового Модельного закона МПА СНГ с изменённым названием «Об информации, информатизации и обеспечении информационной безопасности». Отметим, публичность проводившейся работы: в процессе разработки пояснительная записка и материалы готовившегося законопроекта публиковались для обсуждения на страницах журнала «Информация и связь», обсуждались на научно-практических конференциях в Беларуси и России [11, с. 14–16; 12, с. 11–16].

Подготовленные законопроекты прошли комплексную экспертизу в парламентах государств Содружества и были приняты на 41-й сессии МПА СНГ в ноябре 2014 г. Проект документа «Стратегия обеспечения информационной безопасности государств – участников Содружества Независимых Государств» был направлен для рассмотрения в установленном порядке в Исполкоме СНГ с перспективой подготовки новых межгосударственных программ сотрудничества в сфере безопасности [13, с. 27–57]. Уже в текущем году в Исполкоме СНГ прошло заседание экспертной группы по согласованию проекта этого документа, на котором он был одобрен и признана целесообразной подготовка Решения Совета глав правительств СНГ об утверждении Стратегии обеспечения информационной безопасности.

Важным направлением в совместной работе проводимой российскими и белорусскими учёными являются исследования по тематике правового института тайн [14, с. 54–59]. Законодательное регулирование не может обойти сферу защиты государственной тайны, которая хотя и отражается на степени открытости государства перед обществом, тем не менее, является важным и необходимым элементом обеспечения суверенитета и безопасности государства [15, с. 31–33]. Острота этой

проблематики сегодня возрастает. В национальных законодательствах государств – участников СНГ в настоящее время представлены четыре законодательные модели, законы: «О государственных секретах», «О государственной тайне», «О государственной и служебной тайне» и «О защите государственных секретов» со своим понятийным аппаратом [16]. Это обстоятельство только подчёркивает актуальность сравнительных исследований, совместно проводимых российскими и белорусскими учёными. Планами МПА СНГ на 2015 – 2016 годы предусмотрены разработка Комментария к принятому в 2003 году Модельному закону СНГ «О государственных секретах» и подготовка рекомендаций по его совершенствованию [17, с. 99].

Материалы и наработки всех вышеназванных проектов многократно докладывались и обсуждались на ежегодном теоретическом семинаре сектора информационного права в ИГП РАН в Москве; на научно-практических конференциях: «Теоретические и прикладные проблемы информационной безопасности» и «Информационная безопасность как составляющая национальной безопасности государства» в Республике Беларусь в г. Минске; на конференциях «Информационная безопасность Регионов России» и «Региональная информатика» в Санкт-Петербурге; на секциях национального ИНФОФОРУМА по информационной безопасности, на ежегодной международной научно-практической конференции «Право и информация» в Президентской библиотеке, публиковались в научных изданиях. За прошедший период членами авторского коллектива только в ведущих научных журналах было опубликовано более двух десятков совместных научных публикаций, подготовлены и защищены две докторские диссертации [18], [19].

Заключение. В заключение следует отметить, что проводимая коллективом специалистов России и Беларуси многоплановая работа по проблемам правового обеспечения процессов информатизации на современном этапе освоения потенциала ИКТ и обеспечения информационной безопасности приобретает все большее значение в аспекте гармонизации и совершенствования информационного законодательства. Модельные законы международного сотрудничества Содружества Независимых Государств имеют большое значение для сближения, унификации национальных законов и соответствия их быстро развивающимся процессам электронизации (цифровизации) мира. Сложившееся неформальное сотрудничество российских и белорусских учёных оказалось весьма плодотворным. Работы коллектива российских и белорусских учёных получили высокую оценку, их авторы были отмечены высокими парламентскими наградами.

СПИСОК ЛИТЕРАТУРЫ

1. Бондуровский В.В., Вус М.А., Макаров О.С. СНГ: Информационная безопасность // История. Политика. Право. – 2012, №3-4.
2. Бондуровский В.В., Бачило И.Л., Вус М.А., Кучерявый М.М., Макаров О.С. Парламентское измерение информационной безопасности в рамках СНГ и ОДКБ на современном этапе // Информатизация и связь. – 2014, №3.
3. Бачило И.Л., Бондуровский В.В., Вус М.А., Кучерявый М.М., Макаров О.С. О совершенствовании и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности // Информационное право. – 2013, №1(32).
4. Юсупов Р.М., Шишкин В.М. Информационная безопасность и кибербезопасность: семантический конфликт или сосуществование // Информатизация и связь. – 2012, №9.
5. Вус М.А., Кучерявый М.М., Шакин Д.Н., Юсупов Р.М. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности // Информатизация и связь. – 2012, №9.
6. Информационный бюллетень МПА СНГ. – 2013. №57, Часть 2.
7. Словарь-справочник терминов и определений понятий модельного законодательства государств – участников СНГ / Под ред. М.А. Вуса и В.В. Бондуровского. – СПб.: Изд-во «Юридический Центр – Пресс». 2012. – 360 с.
8. Лепёхин А.Н. О некоторых аспектах разработки и реализации административных регламентов в сфере информационной безопасности // Информатизация и связь. – 2014, №3.
9. Вус М.А., Лепёхин А.Н., Перевалов Д.В. К вопросу предупреждения использования открытых телекоммуникационных серей в террористических и иных противоправных целях // Информатизация и связь. - 2013, №1.
10. Информационный бюллетень МПА СНГ. – 2014. №60, Часть 2.
11. Бачило И.Л., Вус М.А., Макаров О.С. Об изменении Модельного закона СНГ «Об информатизации, информации и защите информации» (2005 г.) в его новой редакции с измененным названием «Об информации, информатизации и обеспечении информационной безопасности. // Информатизация и связь. – 2014, №3.
12. Бачило И.Л. Проект модельного закона «Об информации, информатизации и информационной безопасности» // Теоретические и прикладные аспекты информационной безопасности: материалы международной научно-практической конференции (Минск, 19.07.2014). – Минск.: Академия МВД , 2015. – 417 с.
13. Информационный бюллетень МПА СНГ. – 2015. №62, Часть 2.
14. Вус М.А. К вопросу о культуре секретности // Информационная безопасность как составляющая национальной безопасности государства: материалы международной научно-практической конференции (г. Минск 11-13.07.2003), Т.1. – Минск.: Ин-т нац. безопасности Респ. Беларусь, 2005. – 174 с.
15. Макаров О.С., Вус М.А., Кучерявый М.М. О защите государственных секретов в ОДКБ // Информатизация и связь. – 2013, №6.
16. Глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ. Сборник / Сост.: Бачило И.Л., Вус М.А., Гусев В.С., Макаров О.С. – СПб.: СПИИРАН, 2011. – 79 с.
17. Информационный бюллетень МПА СНГ. – 2014. № 59.
18. Макаров О.С. Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств – участников Содружества Независимых Государств / Автореферат дисс. докт. юр. наук. – М, ИГП РАН, 2014. – 52 с.
19. Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира. / Автореферат дисс. докт. полит. наук. – СПб, СПбГУ, 2014. – 48 с.

УДК 37.047
ГРНТИ 78.21.13

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА И БЕЗОПАСНОСТИ СПЕЦПОДРАЗДЕЛЕНИЙ СИЛОВЫХ ВЕДОМСТВ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ В СИСТЕМАХ ИНЖЕНЕРНОЙ РАЗВЕДКИ МЕТОДА СОГЛАСОВАНИЯ СЛУХОВОГО АНАЛИЗАТОРА ОПЕРАТОРА С АКУСТИЧЕСКИМ КАНАЛОМ

Бобонец Сергей Алексеевич[1], Кузнецов Игорь Викторович[1], Примакин Алексей Иванович[2],
[1]Санкт-Петербургский военный институт внутренних войск МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
[2]Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
e-mails: sbobon@mail.ru, kuznetsov-inz@mail.ru, a.primakin@mail.ru

Аннотация: В статье представлены результаты многолетних исследований, проводимых сотрудниками кафедры обеспечения служебно-боевой деятельности внутренних войск Санкт-Петербургского военного института ВВ МВД России и кафедры специальных информационных технологий Санкт-Петербургского университета МВД России.
Предложен метод согласования слухового анализатора оператора с акустическим каналом систем инженерной разведки; разработаны алгоритмы быстрых процедур в акустической системе обнаружения и идентификации взрывоопасных предметов (ВОП), алгоритмы программ проведения имитационного моделирования и проведения экспериментов по обоснованию технических требований к системам обнаружения и идентификации ВОП.
Полученные результаты позволили повысить эффективность поиска и идентификации в грунтах ВОП акустическими системами инженерной разведки.
Все технические решения испытывались и оценивались при помощи имитационного и натурного экспериментов.

Ключевые слова: *система обнаружения и идентификации взрывоопасных предметов; метод согласования слухового анализатора оператора с акустическим каналом; имитационное моделирование.*

PROVIDING INFORMATION SUPERIORITY AND SAFETY OF SPECIAL FORCES OF POWER DEPARTMENTS BY MEANS OF APPLICATION IN SYSTEMS OF ENGINEERING INVESTIGATION OF THE METHOD OF COORDINATION OF THE ACOUSTIC ANALYZER OF THE OPERATOR WITH THE ACOUSTIC CHANNEL

Bobonets Sergey Alekseevich[1], Kuznetsov Igor Viktorovich[1], Primakin Alexey Ivanovich[2],
[1]St. Petersburg military institute of internal troops of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
[2]Ministry of Internal Affairs St. Petersburg university of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
e-mails: sbobon@mail.ru, kuznetsov-inz@mail.ru, a.primakin@mail.ru

Abstract: Results of the long-term researches conducted by the staff of chair of ensuring office and fighting activity of internal troops of the VV Ministry of Internal Affairs St. Petersburg military institute of Russia and chair of special information technologies of the Ministry of Internal Affairs St. Petersburg university of Russia are presented in article.
The method of coordination of the acoustic analyzer of the operator with the acoustic channel of systems of engineering investigation is offered; algorithms of fast procedures in the speaker system of detection and identification of explosive subjects (VOP), algorithms of programs of carrying out imitating modeling and carrying out experiments for justification of technical requirements to systems of detection and identification of VOP are developed.
The received results allowed to increase efficiency of search and identification in VOP soil speaker systems of engineering investigation.
All technical solutions were tested and estimated by means of imitating and natural experiments.

Keywords: *system of detection and identification of explosive subjects; method of coordination of the acoustic analyzer of the operator with the acoustic channel; imitating modeling.*

В статье представлены результаты многолетних исследований, проводимых сотрудниками кафедры обеспечения служебно-боевой деятельности внутренних войск Санкт-Петербургского военного института ВВ МВД России и кафедры специальных информационных технологий Санкт-Петербургского университета МВД России.

Предложен метод согласования слухового анализатора оператора с акустическим каналом систем инженерной разведки; разработаны алгоритмы быстрых процедур в акустической системе обнаружения и идентификации взрывоопасных предметов (ВОП), алгоритмы программ проведения имитационного моделирования и проведения экспериментов по обоснованию технических требований к системам обнаружения и идентификации ВОП.

Полученные результаты позволили повысить эффективность поиска и идентификации в грунтах ВОП акустическими системами инженерной разведки.

Все технические решения испытывались и оценивались при помощи имитационного и натурного экспериментов.

Одной из актуальных проблем, стоящих перед силовыми структурами, является разработка новых средств обнаружения ВОП, что обеспечивало бы информационное превосходство при проведении контртеррористических операций спецподразделениями силовых ведомств.

На первом этапе исследования был проведен сравнительный анализ литературных и патентных материалов по существующим методам обнаружения ВОП [1], результаты которого показали, что в подавляющем большинстве случаев разработчики технических систем поиска в качестве оконечного звена используют слуховой анализатор человека (САЧ). Опыт применения систем поиска ВОП показывает, что ни одна техническая приемная система не может сравниться с эффективностью слуховой системы человека по динамическому диапазону, помехоустойчивости и возможности идентификации объектов поиска. Примерами таких устройств являются: приборы поиска инженерных мин и ВОП (миноискатели различного принципа действия), в которых слух человека выступает, как приёмная система акустических сигналов.

Поэтому задачей проведенного научного исследования являлась разработка метода согласования слухового анализатора оператора с сигналами, поступающими от датчиков акустических поисковых систем инженерной разведки, что обеспечило бы повышения эффективности работы поисковых элементов (ПЭ).

Эффективность функционирования поисковых систем зависит от природы физического явления заложенного в ПЭ, от методов представления снятого с ПЭ сигнала и согласования выходного сигнала ПЭ с САЧ. Ввиду того, что в большинстве ПЭ используется эффект магнитостататики намагниченных тел, проведена оценка напряженности магнитного поля от объекта поиска.

Получено решение для общего случая, когда внешнее магнитное поле имеет произвольное направление по отношению к осям эллипсоида [2]. В рассмотренном способе обнаружения полезный сигнал быстро убывает с увеличением расстояния до тела. Поэтому целесообразно было рассмотреть другой способ обнаружения, а именно индукционный метод выделения сигнала. Наведённая ЭДС в данном способе убывает с увеличением расстояния до тела гораздо медленнее, чем в предыдущем способе.

Общая схема обработки сигналов современными металлоискателями представлена на рисунке 1.

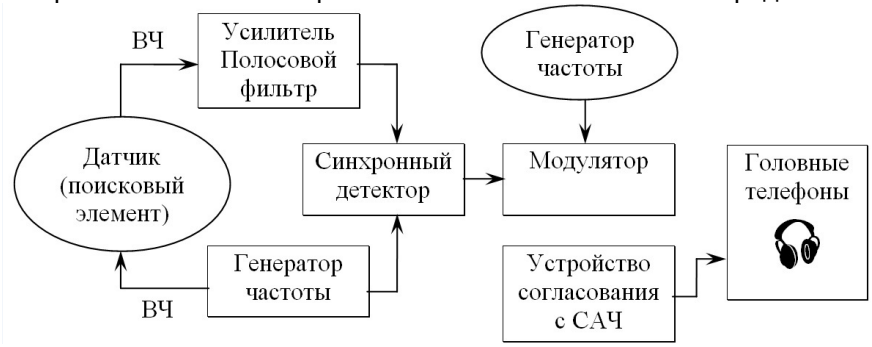


Рис. 1. Общая схема обработки сигналов в металлоискателях

Здесь сигнал на входе датчика переносится из области низких частот в область высоких частот, затем усиливается и обрабатывается.

Откликом системы является сигнал, формируемый на выходе синхронного детектора в виде низкочастотного колебания. При этом свойства выходного сигнала отражают природу объекта поиска. При поиске ВОП в основе процедуры функционирования поисковой системы, как правило, лежит метод синхронного детектирования. В металлоискателях для согласования низкочастотных колебаний с САЧ низкочастотный процесс на выходе синхронного детектора модулируется тоном. Результат модуляции прослушивается с помощью головных телефонов.

С учетом требования получения большей по объему информации о частотно-временных свойствах поля объекта предлагалось использовать синхронное детектирование с разверткой [3].

Схема поисковой системы представлена на рисунке 2.

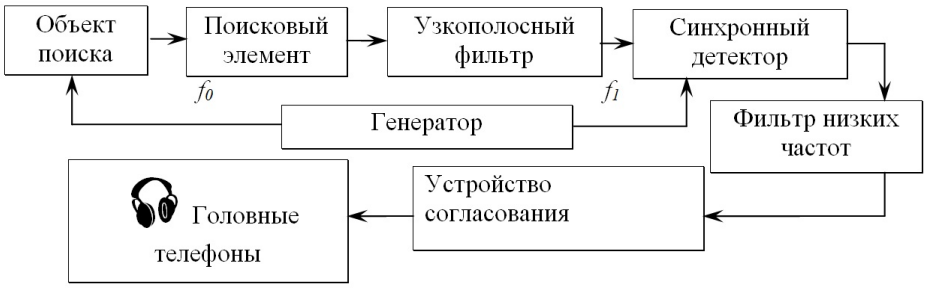


Рис. 2. Концептуальная схема функционирования поисковой системы

Она содержит: датчик (поисковый элемент), фиксирующий параметры физического явления; генератор гармонических колебаний с частотой f_0; фильтр; синхронный детектор и полосовой фильтр на низких частотах; устройство согласования.

Сигнал от генератора взаимодействует с сигналом от объекта поиска, и результат взаимодействия поступает на вход датчика, который реализует измерение явления на частотах в пределах полосы сигнала. С выхода датчика сигнал поступает на вход полосового фильтра и затем – на вход синхронного детектора, фильтр низких частот и затем на устройство согласования с САЧ, эволюция которого сформировала зону эффективного приема в диапазоне от 200 Гц до 4000 Гц.

Был предложен метод синхронного детектирования с разверткой. В основе метода положено условие: генератор сигнала имеет модуляцию частоты, например, по закону линейно-частотной модуляции (ЛЧМ).

Преимущество синхронного детектора с разверткой по сравнению с синхронным детектором с постоянной частотой в том, что в области взаимодействия физического явления с датчиком формируется набор частот. Поэтому, если явление частотно зависимо, то отклик на выходе датчика тоже будет частотно зависим, а это дает дополнительную информацию для классификации объекта оператором. Для повышения эффективности функции поискового элемента предлагается использовать для прослушивания сигналы бинаурально с двух независимых датчиков с различной ориентацией элементов в пространстве.

Однако, для окончательного решения этого вопроса необходимо было провести большой объем экспериментальных исследований по оценке пороговых характеристик слуха при восприятии им широкополосных сигналов, в том числе, при использовании бинаурального прослушивания сигналов.

В последнее время, при анализе САЧ, принимают теоретико-групповой подход. Суть этого подхода – исследование преобразований сигналов, не изменяющих эффективность слуха в достаточно широких пределах вариации их параметров. Так же полагается, что процесс выбора преобразований диктуется физическими условиями процесса передачи энергии в акустическом канале. Такой подход позволяет по-новому осмыслить ряд задач физиологической акустики и предложить ряд практических решений по технике согласования САЧ со слуховыми трактами различных устройств. Теоретико-групповой подход позволил провести классификацию базовых сигналов для восприятия САЧ [4].

Для согласования акустических сигналов со слуховым анализатором оператора предложен ряд инженерных решений, позволивших оптимизировать задачу слухового приема. Так, например, предлагались операции транспонирования сигналов и комбинация операций транспонирования и гетеродинирования сигналов [5].

Известно, что САЧ, как приемник сигналов, реализует эффективную обработку не только в определенном диапазоне частот, но и с определенными размерами масштабов (количеством волн) сигналов. По-видимому, причина этого факта заключается в том, что исходя из ограничения размера «частотно-временного окна» когерентной обработки сигнала для акустического канала, САЧ не имело смысла формировать правило обработки сигналов с размерами, превосходящими имеющийся размер для среды. Поскольку инвариантом частотно-временного «размера» является количество волн, в экспериментальных исследованиях исследовались оценки вероятностных характеристик САЧ в функции количества волн. Ранее проводимые экспериментальные исследования для тонально-импульсных сигналов показали, что эффективный прием слуховой системы достигается при обнаружении сигналов в диапазоне 100–4000 Гц с количеством 32–128 полных колебаний (волн) [6]. Указанную частотно-временную область называют областью эффективного приема САЧ.

Следующим шагом было изучение эллиптической симметрии, обусловленной одновременным изменением масштаба, сдвига и инверсии. Эту симметрию в акустике слуха называют динамической симметрией [7].

Для проведения экспериментальных исследований в программной математической системе MathCAD был разработан цифровой аудиометр. Методика эксперимента на аудиометре заключалась в требовании обнаружения оператором на фоне шумовой помехи гиперболических сигналов с

различной относительной полосой в условиях моноурального и бинаурального приемов [8]. Сформированные сигналы с помехой «предъявлялись» слуховой системе оператора через головные телефоны (наушники).

Разработанный алгоритм и методика позволяли обучать испытуемых не только обнаружению сигналов, но и стабилизации слуховых функций на индивидуальных пороговых уровнях. Это достигалось тем, что в процессе обучения испытуемому сообщалась информация о правильности или ошибочности его реакции.

Сравнительный анализ экспериментальных данных показал: наиболее эффективный прием для САЧ осуществляется для гиперболических сигналов с большой меллиновской частотой (больше 100), т.е. для сигналов, приближающихся к тональным сигналам; бинауральный прием САЧ эффективнее моноурального приема сигналов; наиболее эффективный прием у САЧ достигается для сигналов в диапазоне 32–64 волн.

Полученные экспериментальные данные имеют большое практическое значение т.к. позволили выбрать параметры сигналов, обеспечивающих их наилучший бинауральный прием.

Для оценки дальности обнаружения целей (объектов) исследовался частотный диапазон принимаемых сигналов. В области низких частот (НЧ) явление поглощения имеет меньшее влияние на сигнал, чем в области высоких частот. Кроме того, НЧ сигналы могут огибать препятствия, имеющие малые волновые размеры. Но эволюционно у САЧ не было необходимости вырабатывать эффективные свойства функционирования в этом диапазоне частот. Поэтому исследовалась возможность приема сигналов низкочастотного диапазона слуховой системой путем их переноса (транспонирования) в эффективный диапазон восприятия САЧ. Целью эксперимента было выявление порогового значения входного отношения сигнал/шум (S/N), при котором САЧ обнаруживает транспонированные сигналы. Исследование проводилось с помощью цифровой акустической системы при реализации алгоритмов с помощью комплекса программ в математической среде MathCAD.

Целью эксперимента было выявление порогового значения входного отношения сигнал/шум (S/N), при котором САЧ обнаруживает транспонированные сигналы. Исследование проводилось с помощью цифровой акустической системы при реализации алгоритмов с помощью комплекса программ в математической среде MathCAD.

Методической особенностью этой серии экспериментов являлось использование информационных мер Кульбака и Шеннона. Эффективность обнаружения рассматривалась как оценка пропускной способности канала. Рассмотрение информационных мер позволяет судить о потерях информации в канале.

Полученные результаты, позволили сделать вывод о том, что для эффективной работы САЧ в наиболее благоприятном частотном диапазоне значение S/N должно лежать в интервале $d = 32 \div 40$.

Данный эксперимент дает исходные данные для выработки требуемого отношения S/N. Эксперимент показал, что обнаружитель может эффективно работать при согласовании воспроизводимых сигналов с САЧ, т.е. при перенесении сигнала в эффективный диапазон восприятия слуховой системой.

Сигнал от ПЭ имеет сложную фазовую структуру и его эффективность восприятия САЧ может не совпадать с прогнозом данных полученных при восприятии тональных сигналов. Для устранения пробела в экспериментальных данных в работе был поставлен и проведён эксперимент по оценке слуховой функции САЧ в зависимости от фактора когерентности принимаемых сигналов [9].

Сигнал имел гармоническое заполнение. Задавалась частота дискретизации сигнала f_d. Сигнал представлял собой последовательность случайных отрезков с переменным количеством волн и переменным чередованием пустых промежутков, но в одном случае фазовая структура такого сигнала не нарушалась, а в другом начальная фаза задавалась случайным механизмом.

Постановку задачи исследования можно объяснить следующим: целесообразно ли использование генератора, который сохраняет начальную фазу или генератор может формировать питание поискового элемента с произвольной начальной фазой. Критерием принятия того или иного решения является эффективность восприятия указанных сигналов САЧ.

Экспериментально доказано, что когерентный прием сигналов (с сохранением фазы) более эффективен для обнаружения объектов, чем в случае формирования сигналов с флюктуирующей фазой. Наиболее эффективный прием САЧ осуществляет на частоте 690 Гц.

С увеличение количества волн имеет место ухудшение эффективности приёма на всех частотах, но наиболее явно это проявляется на высоких частотах.

Разработанный метод согласования сигналов от объектов военного назначения со слуховым каналом показал:

– для повышения эффективности метода синхронного детектирования в поисковых системах, целесообразно применять специальные модулирующие сигналы, позволяющие получить более полную информацию о признаках объекта поиска и более полного учета среды;

– для повышения эффективности поисковых систем предлагается сигналы с выхода синхронного детектора представлять САЧ согласованными с областью эффективного приема анализатора. Для реализации процедуры согласования предлагается вместе с операцией гетеродинирования применять операцию транспонирования низкочастотных сигналов;

Акустический эксперимент, проведенный для оценки области эффективного приема САЧ, показал, что область эффективного приема при восприятии частотно-модулированных сигналов гиперболического типа лежит в диапазоне количество волн сигнала от 32 до 64;факт зависимости области эффективного приема от количества волн средней частоты сигнала f_0 в диапазоне $f_0 \in (300 \div 2000)$ Гц является естественным. Расчеты показали, что процедура согласования сигналов с областью эффективного приема позволит поднять помехоустойчивость системы обнаружения в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов И.В., Примакин А.И. Сравнительный анализ существующих методов обнаружения взрывоопасных предметов при проведении контртеррористических операций / Вестник Санкт-Петербургского университета МВД России, №4 (44), 2009, С.99–103.
2. Примакин А.И. Методика и результаты экспериментальных исследований по передаче аудиосигнала в акустическом канале с учетом его масштабно-временных характеристик. / Вестник Санкт-Петербургского университета МВД России, 2002, №2 (14), С.187–193.
3. Ковалевский Н.Г., Кузнецов И.В., Примакин А.И. Обеспечение информационной безопасности действий войск посредством применения акустической системы обнаружения и классификации объектов военного назначения. Труды V Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2007). СПб., 2008, С.180–182.
4. Примакин А.И. Особенности восприятия речевых сигналов слуховым анализатором человека по защите информации при целенаправленных помехах. Вестник Санкт-Петербургского университета МВД России. 2002, №3 (15), С.196–199.
5. Примакин А.И. Алгоритмы вэйвлет-преобразования и обработки передаваемой по каналам связи информации с целью ее сжатия и обеспечения безопасности. VIII Санкт-Петербургская международная конференция «Региональная информатика-2002 («РИ-2002»), СПб, 26–28 ноября 2002.: Материалы конференции, СПб, 2003, С.194–195.
6. Ковалевский Н.Г., Примакин А.И. Метод обнаружения доплеровской модуляции акустических колебаний Материалы IV Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2005)», Санкт-Петербург, 2005, С.60–61
7. Примакин А.И. Исследование масштабно-временных характеристик акустического канала связи для обеспечения информационной безопасности, передаваемых по нему аудиосигналов. / Морской сборник, №11, 2003, С.18–25.
8. Ковалевский Н.Г., Кузнецов И.В., Примакин А.И. Повышение эффективности работы систем обнаружения и идентификации посредством метода согласования слухового анализатора оператора с акустическими сигналами от объекта поиска. / Труды XI Санкт-Петербургской международной конференции «Региональная информатика – 2008», СПб., 2009, С.50–52.
9. Кузнецов И.В. К вопросу о слуховой функции человека при обнаружении сигналов в зависимости от фактора когерентности. / Материалы 17 межвузовской научно-технической конференции ВМИРЭ им. А.С. Попова, Петродворец 2007, С.211–213.

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕРРИТОРИЯМИ «БЕЗОПАСНЫЙ ГОРОД»

Жигадло Валентин Эдуардович,
ЗАО «Институт телекоммуникаций»,
Россия, Санкт-Петербург, ул. Кантемировская, д. 5
e-mail: zve@mail.ru

Аннотация: В статье рассмотрены автоматизированная информационная система (АИС) управления территориями «Безопасный город», ее задачи, функциональные подсистемы, объекты управления, и единая межведомственная интегральная автоматизированная ИС (МИАИС) «Интеллектуальный город»

Ключевые слова*: автоматизированная информационная система; система информатизации; межведомственная интегральная автоматизированная информационная система*

AUTOMATED INFORMATION MANAGEMENT SYSTEM TERRITORY OF THE "SAFE CITY"

Zhigadlo Valentin,
JSC «Institute of Telecommunications»
Russia, St. Petersburg, ul. Kantemirovskaya, d. 5
e-mail: zve@mail.ru

Abstract: This article describes the automated information system (AIS) management of territories "Safe City", its objectives, functional subsystems, facilities management, and uniform interdepartmental integrated automated IP (MIAIS) "Smart City"

Keywords: *automated information system; system information; interdepartmental integrated automated information system*

Современное развитие информационного общества характеризуется интенсивным внедрением автоматизированных информационных систем (АИС), направленных на повышение эффективности управления различными сферами, как экономики так и городского хозяйства, а также 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.

Проведенный анализ развития информационного общества в Санкт-Петербурге за последние 5 лет позволяет выделить следующие направления его развития, отмеченные в проекте программы «РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В САНКТ-ПЕТЕРБУРГЕ НА 2013-2016 ГОДЫ»:

– повышение качества государственного управления за счет внедрения современных информационных технологий (развитие электронного правительства);

– обеспечение решения задач развития технической и технологической основы становления информационного общества, доступа граждан и организаций к услугам на основе информационных технологий;

– обеспечение решения задач предупреждения угроз, возникающих в информационном обществе, создание средств защиты информации, мониторинг угроз, регулярная оценка защищенности компонентов инфраструктуры, ликвидация неблагоприятных последствий нарушения ее защиты, своевременная модернизация систем защиты компонентов инфраструктуры;

– информатизация жилищно-коммунального хозяйства;

– информатизация сферы медицинского обслуживания и социального обеспечения населения;

– информатизация сферы культурного и гуманитарного просвещения;

– внедрение спутниковых навигационных технологий (GPS, ГЛОНАСС) в целях социально-экономического развития Санкт-Петербурга;

– информатизация в области транспорта и связи;

– использование информационных и телекоммуникационных технологий в образовании, в развитии науки, техники и подготовки квалифицированных кадров в сфере информационных и телекоммуникационных технологий.

– Модернизация и развитие телекоммуникационной инфраструктуры

– Создание единого РЦОД

К данному перечню направлений, сформулированных, несомненно, своевременно, необходимо добавить совокупность задач по мониторингу и прогнозу техногенных ситуаций, предупреждению угроз техногенных катастроф в рамках интегрированной автоматизированной информационной системы (ИАИС) «Безопасный город», или «Безопасная территория».

За прошедший пятилетний период в Санкт-Петербурге Комитетом по связи и информатизации (КИС) реализован целый ряд довольно крупных проектов, в том числе:

– строительство и ввод в эксплуатацию Единой Мультисервисной Телекоммуникационной Сети исполнительных органов государственной власти Санкт-Петербурга (ЕМТС);

– внедрение и развитие Автоматизированной информационной системы «Обеспечение безопасности жизнедеятельности Санкт-Петербурга»;

– внедрение системы межведомственного электронного взаимодействия Санкт-Петербурга (СМЭВ СПб);

– завершение создания и эксплуатация межведомственной автоматизированной информационной системы предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде (МАИС «Электронные услуги СПб»)»;

– развитие Автоматизированной информационной системы бюджетного процесса - электронного казначейства (АИСБП-ЭК);

– развитие Автоматизированной информационной системы «Городской заказ»;

– развитие автоматизированной системы управления единой дежурной службы (АСУ ЕДС) Администрации Санкт-Петербурга;

– развитие Интегрированной системы информационно-аналитического обеспечения деятельности исполнительных органов государственной власти Санкт-Петербурга (ИС ИАО) – системы поддержки принятия управленческих решений руководством города;

– проектирование, разработка и внедрение базовых компонентов Единой системы учета населения Санкт-Петербурга (ЕСУН);

– внедрение и развитие Автоматизированной системы «Электронный социальный регистр населения»;

– развитие территориальной отраслевой региональной информационной системы (ТОРИС);

– создание системы защиты информации в исполнительных органах государственной власти;

– реализация системы периодической переподготовки сотрудников исполнительных органов государственной власти Санкт-Петербурга в области применения современных информационных

технологий, развитие системы дистанционного обучения в сфере высшего профессионального образования;

– создание системы защиты информации, составляющей государственную тайну, от утечки по техническим каналам и от технических разведок в Администрации Санкт-Петербурга (в Смольном);

– создание системы защиты информации ограниченного доступа в информационных и телекоммуникационных сетях и системах исполнительных органов государственной власти Санкт-Петербурга.

Вместе с тем, существует ряд проблем, сложившихся исторически и препятствующих повышению эффективности использования информационных технологий в целом, которые носят комплексный межведомственный характер и не могут быть решены на уровне отдельных органов государственной власти. Устранение этих проблем требует значительных ресурсов, скоординированного проведения организационных изменений и обеспечения согласованности действий органов государственной власти.

В результате недостаточного комплексного подхода к решению задачи формирования и развития информационного общества, как одного из необходимых этапов модернизации экономики, проявляются негативные тенденции, которые при сохранении текущей экономической ситуации могут усиливаться.

Наиболее существенными из обозначенных негативных тенденций являются:

1. Результаты разработки и внедрения информационных технологий, проводящихся по заказу отдельных органов государственной власти, не всегда носят системный характер, в частности:

– внедрение средств информационных технологий носит преимущественно локальный, ведомственный характер, отсутствует системная интегративная проработка задач построения информационных систем различного назначения;

– недостаточными темпами развиваются инфраструктура создаваемых информационных систем и инфраструктура доступа населения к сайтам органов государственной власти и другие средства информационно-справочной поддержки и обслуживания населения;

– отсутствуют системные проработки унифицированных форм и форматов хранения данных (на базе РЦОД), единых форматов доступа к данным, унифицированных интерфейсов доступа пользователей к набору информационных систем;

– отсутствуют проработки создания системообразующих информационных систем, обеспечивающих унифицированный доступ к функционально связанному, в рамках всех информационных систем или отдельных сфер жизни города, наборам услуг, таких как, ИС «Безопасный город», ИС «Открытый город», ИС «Интеллектуальный город»;

– отсутствует проработка вопроса унификации сбора исходных данных о состоянии различных отраслей городского хозяйства на базе, например, унифицированного набора сетей сенсоров (в областях: транспорт, услуги, связь, кризисные ситуации, ОБЖ, строительство и жилищно-коммунальное хозяйство, медицинское обслуживание и социальное обеспечение населения МВД, МО, МЧС и т.д.);

– отсутствует необходимая нормативная правовая база, а также стандарты и регламенты предоставления органами государственной власти требуемой информации населению, организациям и другим органам государственной власти, не сформирована инфраструктура, обеспечивающая информационную безопасность электронных форм взаимодействия органов государственной власти между собой, а также с населением и организациями, для электронных форм взаимодействия не реализованы такие услуги, как нотариальные услуги в электронном виде, официальная публикация электронных документов и другие услуги, аналогичные услугам при традиционных формах взаимодействия на основе использования бумажных документов.

2. Слабо координируется использование органами государственной власти информационных технологий, недостаточно используется лучший опыт внедрения информационных технологий для повышения эффективности государственного управления, в частности:

– наблюдается несовместимость программно-технических решений, невозможность обмена данными между различными государственными информационными системами, отсутствуют механизмы и технологии оперативного информационного взаимодействия федеральных и региональных информационных систем между собой и друг с другом;

– существуют различия между органами государственной власти по использованию информационных технологий в своей деятельности;

– не все органы государственной власти Санкт-Петербурга использует комплексные системы электронного документооборота;

– не автоматизированы процедуры сбора и обработки информации, необходимой для планирования и определения целевых показателей деятельности органов государственной власти;

– отсутствуют решения и стандарты в области обмена данными в электронном виде на межведомственном уровне, а также с населением и организациями, что становится особенно актуальным по мере дальнейшего развития государственных информационных систем;

– по-прежнему остается недостаточным уровень компьютерной грамотности государственных и муниципальных служащих, что предопределяет актуальность организации непрерывного обучения государственных служащих и оценки навыков использования информационных технологий в ходе предусмотренной законом периодической аттестации;

– недостаточными темпами развиваются инфраструктура создаваемых информационных систем и инфраструктура доступа населения к сайтам органов государственной власти и другие средства информационно-справочной поддержки и обслуживания населения:

– не автоматизированы процедуры сбора и обработки информации;

– недостаточными темпами развиваются средства информационно-справочной поддержки и обслуживания населения;

– не сформирована инфраструктура, обеспечивающая информационную безопасность электронных форм взаимодействия органов государственной власти между собой, с населением и организациями, отсутствуют доступные механизмы обеспечения доверия к электронной цифровой подписи, не создана целостная система удостоверяющих центров и их услуги не являются массовыми.

3. Сохраняется отставание рынка информационных технологий, недостаточно быстрыми темпами происходит становление экономики, осуществляемой с помощью информационных технологий.

4. Сохраняется высокий уровень различия в использовании информационных технологий различными слоями общества, и недостаточно развита базовая инфраструктура информационного общества, в частности:

– уровень различия в использовании информационных технологий в домашних хозяйствах является высоким;

– сохраняются проблемы организации широкополосного доступа для конечных пользователей и низкие показатели качества доступа к сети Интернет.

5. Возрастают угрозы безопасности в информационном обществе, в том числе:

– одной из угроз является увеличение количества компьютерных преступлений, возросла их корыстная направленность, а также наносимый материальный ущерб, увеличилось количество трансграничных компьютерных преступлений, совершенных группами лиц;

– информационные технологии все чаще используются для совершения традиционных преступлений, в частности хищений, вымогательств, мошенничества и террористической деятельности.

6. Отсутствуют проработки создания системообразующих информационных систем, обеспечивающих унифицированный доступ к функционально связанному, в рамках всех информационных систем или отдельных сфер жизни города, набору услуг.

7. Отсутствует необходимая нормативная правовая база, а также стандарты и регламенты предоставления органами государственной власти требуемой информации населению, организациям и другим органам государственной власти.

8. Не достаточный уровень качества подготовки специалистов в области ИТ.

В целом, существующая структура построения системы предоставления информационных услуг (система информатизации), призванная объединить все созданные ИС, строится по аддитивному принципу, объединяя разнородные ИС через единую транспортную сеть и обеспечивая единственную возможность доступа к выделенному набору услуг, как населению, так и ОГВ, через инфраструктуру созданной ЕМТС. Такой подход на данном этапе позволяет обеспечить удаленный доступ к набору ИС, но порождает при этом проблему связанную с эволюционным ростом числа ИС и, как следствие, приводящую к усложнению абонентского интерфейса доступа и росту числа клиентских приложений, что, по сути, представляет собой тупиковый путь развития.

Проводя анализ достигнутых результатов в области создания ИС, следует отметить, что наиболее значимыми из выше перечисленных ИС, реализованных под руководством КИС и имеющими системные признаки в архитектуре построения, являются: Единая Мультисервисная Телекоммуникационная Сеть исполнительных органов государственной власти Санкт-Петербурга (ЕМТС), обеспечивающая единую защищенную транспортную основу для всех существующих и создаваемых ИС, межведомственная автоматизированная информационная система предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде (МАИС «Электронные услуги СПб»)(МАИС МФЦ) и Автоматизированная информационная система «Обеспечение безопасности жизнедеятельности Санкт-Петербурга».

МАИС «Электронные услуги СПб» представляет собой единственную ИС, созданную по системным принципам, обладающую такими свойствами, как масштабируемость, расширяемость, модульность и поддерживающую единый унифицированный клиентский интерфейс ко всему поддерживаемому набору госуслуг (Рис. 1).

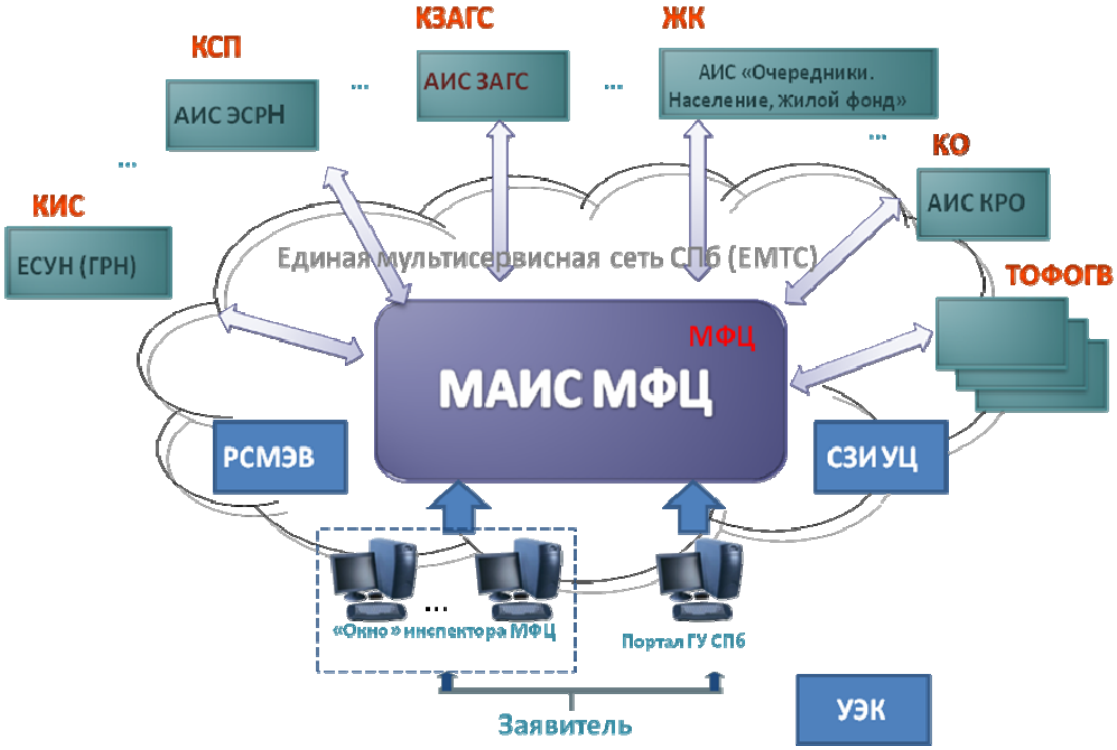


Рис. 1. Структура МАИС МФЦ

Одной из ключевых ИС является также АИС ОБЖ (Рис. 2), однако ее текущая реализация не лишена ряда существенных недостатков, таких как:

– сужен функциональный состав задач до контроля ПДД, видеонаблюдения, без парсинга контента, и контроля радиационной обстановки, с элементами обратной связи с населением;

– отсутствует интеграция с базами данных оперативных служб силовых структур (МВД, МЧС, ФСО, ФСБ, МО) и самими оперативными службами на уровне взаимодействия ОД и ИС;

– отсутствуют задачи мониторинга состояния и анализа угроз безопасности в сферах бизнеса, связи и финансов, энергетики, инженерных систем города, а также в сфере экологии и ЧС; отсутствуют решения по обеспечению безопасности на стратегических объектах городской инфраструктуры (промышленные и энергетические объекты, инженерные сети, мосты тоннели, транспортные развязки), а также решения по обеспечению безопасности в период массового скопления людей на городских мероприятиях и в период саммитов.

В этой связи представляется целесообразным в качества прообраза единой ИС управления городским хозяйством, построенной на системных принципах и обладающей такими свойствами, как эффективность, масштабируемость и функциональность, рассмотреть создание в Санкт-Петербурге интегрированной автоматизированной системы управления безопасностью жизнедеятельности города, в том числе и в кризисных ситуациях – АИС «Безопасный Город».

Целью АИС «Безопасный Город» является: обеспечение комплексного решения задачи повышения безопасности жизнедеятельности города за счет реализации мероприятий по мониторингу и предупреждению угроз, возникающих в регионе и информационном обществе, по обеспечению безопасности жизнедеятельности граждан, оперативному и эффективному устранению последствий техногенных и природных катастроф, оптимизации организации взаимодействия экстренных оперативных служб и повышению эффективности их реагирования на возникающие угрозы и вызовы населения.

Задачами АИС «Безопасный Город» являются: оперативный сбор и накопление актуальной и достоверной информации о чрезвычайных ситуациях, природных и техногенных катастрофах, террористических актах, состоянии окружающей среды и организация своевременного и полноценного информационного обеспечения процесса подготовки и принятия управленческих решений в области защиты населения и территорий от чрезвычайных ситуаций, террористических актов, природных и техногенных катастроф, а так же предупреждение и ликвидация угроз с использованием комплекса современных информационных технологий наблюдения и моделирования.

Рис.2. Функциональный состав АИС ОБЖ Санкт- Петербурга

Решение «Безопасный город» включает:

– триединую ИС (Рис. 3) - Управления кризисными ситуациями, Противодействия криминалу и терроризму и Городское управление в кризисных ситуациях, объединяемых на базе единой геоподосновы защищенной телекоммуникационной сетью (ЕМТС),

– сеть сенсоров, обеспечивающих мониторинг состояния городского хозяйства, окружающей среды и ситуации в городе и доведение управляющих воздействий до объектов городского хозяйства,

– Городской ситуационный центр, обеспечивающий анализ поступающей информации, прогноз развития сложившейся ситуации и выработку управляющих воздействий по управлению городом, в том числе и в кризисных ситуациях.

Функциональными подсистемами АИС «Безопасный город», позволяющей выполнять моделирование ситуации и прогноз состояния безопасности в городе в едином геоинформационном пространстве, с целью оперативного управления по обеспечению безопасности жизнедеятельности города, являются (Рис. 4.):

– ИС «Социально-активные территории»
– ИС «Городские мероприятия (скопления людей)»
– ИС «Чрезвычайные ситуации (критические объекты)»
– ИС «Погодные условия и экология»
– ИС «Транспорт»
– ИС «Инженерные сети, сети связи»
– ИС «Энергообеспечение»
– ИС «Объекты криминала»
– ИС «Объекты терроризма»

С помощью АИС «Безопасный город» решаются ключевые задачи обеспечения безопасности на объектах повышенного внимания, включая области, лежащие за пределами человеческих возможностей, такие как:

– Комплексный мониторинг и анализ обстановки в городе и поддержка принятия управленческих решений.

– Работа всех взаимодействующих структур (в том числе и силовых) в едином геоинформационном пространстве с едиными исходными данными в реальном времени.

– Обработка информации от большого количества сенсоров и видеокамер в едином геоинформационном пространстве с идентификацией и анализом ситуаций, требующих оперативного вмешательства.

– Получение и отображение видеоданных от малых беспилотных летательных аппаратов в реальном времени на трехмерной электронной карте города.

– Удаленная работа через Web-клиент и локальную сеть с подсистемами ГИС 3D в едином информационном пространстве в реальном времени.

– Возможность интеграции решения с различными типами датчиков: видео, аудио, радиолокационных, гидро- и метеорологических, местоположения мобильных объектов, химических, биологических и радиоактивных.

– Моделирование развития ситуаций по направлениям в геоинформационном пространстве и обеспечение взаимодействия между государственными службами.

– Анализ финансовых рисков и экономических угроз.

Рис. 3.Структура решения «Безопасный город»

Рис. 4. Функциональные подсистемы АИС «Безопасный город»

При этом объектами управления АИС «Безопасный город» являются: ГО и чрезвычайные ситуации, правопорядок и общественная безопасность, стратегические объекты (электростанции, дороги, мосты и тоннели, инженерные сети и системы), окружающая природная среда и экология, промышленность транспорт и связь, экономика, а в качестве средств могут выступать: единая геоподоснова города (ГИС), средства связи и видеонаблюдения, разнообразные сенсоры и датчики (видео, аудио, радиолокационные, гидро- и метеорологические, местоположения мобильных объектов, химические, биологические и радиоактивные), беспилотные летательные аппараты (БПЛА), спутниковые навигационные средства системы ГЛОНАСС.

Архитектура АИС «Безопасный город» (Рис. 5.) должна строиться на системных принципах и обладать такими свойствами, как масштабируемость, расширяемость, модульность, а так же обеспечивать единый унифицированный клиентский интерфейс ко всему набору государственных услуг и реализующих их ИС. Такое построение АИС «Безопасный город» делает ее архитектуру функционально независимой от интегрируемых ИС.

Организующей основой АИС «Безопасный город», обеспечивающей выработку адекватных управленческих решений в кризисных ситуациях, является Ситуационный центр управления, контроля и связи, основными задачами которого являются:

1. Адекватное оперативное отображение ситуации (обработка полученных данных в реальном времени, сопоставление и анализ событий, интеллектуальная поддержка, на основе знаний, анализа и прогноза ситуации в реальном времени).

2. Оперативное отображение и обмен данными, поддержка интерфейса оперативного взаимодействия с органами государственной власти, быстрое доведение объективной информации оперативным службам.

3. Оперативное реагирование на события в городе, основанное на использовании объективной актуальной и всесторонней информации о событии, интеллектуальных средств поддержки принятия решений на основе знаний и средств моделирование развития ситуации в реальном времени.

Рис. 5. Архитектура АИС «Безопасный город»

Автоматизированная система видеонаблюдения, фото- и видео-фиксации, фото- и видео-распознавания, как одна из ключевых систем в наборе сенсоров оперативного сбора информации, должна осуществлять комплекс мер направленных на выявление и предупреждение нарушений Правил дорожного движения (ПДД), а также преступлений и правонарушений.

По линии обеспечения безопасности дорожного движения система видеонаблюдения должна выполнять функции по выявлению и фиксации следующих нарушений ПДД:

– превышение максимальной скорости;
– выезд на полосу встречного движения;
– движение на запрещающий сигнал светофора;
– запрещенная остановка и стоянка;
– запрещенное движение задним ходом;
– нарушение дорожной разметки и правил маневрирования;
– проезд запрещенного типа транспортного средства;
– нарушение правил тонировки;
– нарушение правил пользования ремнями безопасности;
– нарушение правил использования переговорных устройств и иных средств связи;
– нарушение правил перевозки пассажиров;
– использование подложных государственных номерных знаков;
– управление транспортом, находящимся в розыске, с возможностью фиксации и распознавания государственных номерных знаков, а также дорожно-транспортных происшествий, выявления автотранспортных средств, владельцы которых несвоевременно оплатили либо уклоняются от оплаты административных штрафов.

По линии обеспечения общественной безопасности и борьбы с преступностью система видеонаблюдения должна выполнять функции по выявлению и фиксации:

– правонарушений и преступлений, совершенных в общественных местах и на улицах;

– анализ миграционной обстановки, контроль и выявление мигрантов;
– лиц, находящихся в розыске и состоящих на различных учетах;
– нештатных ситуаций.

Система видеонаблюдения также должна осуществлять функции по сбору и анализу дорожной (транспортной) статистики по следующим параметрам:

– общее количество транспортных средств и физических лиц, прошедших через контролируемую зону за определенный временной интервал;
– время регистрации;
– количество транспортных средств каждого типа;
– зафиксированная скорость;
– габариты транспортных средств;
– средняя скорость по всем транспортным средствам;
– средняя скорость движения по типам автомобилей;
– дистанция между транспортными средствами;
– загруженность полосы (%);
– превышение скорости движения;
– движение по встречной полосе;
– остановка и стоянка транспортных средств;
– заторы.

В целях предотвращения наводнений и прогноза сезонной паводковой ситуации система должна обеспечивать:

– Визуальный анализ паводковой ситуации в реальном масштабе времени.
– Выявление опасных зон в городах, выработка рекомендаций по предупреждению и устранению последствий затопления
– Возможность взаимодействия с любыми другими модулями подсистемы для комплексного анализа ситуации.

В целях защиты города от таких стихийных бедствий, как землетрясения, сход селей и лавин система позволяет:

– Выявлять опасные зоны в городах, моделировать возможные последствия и вырабатывать рекомендации по предупреждению и устранению последствий затопления селями.
– Выполнять оценку времени схода селей и лавин, возможного нанесенного ущерба, оценивать возможный размер и площадь возможного ущерба, определять жилые зоны, подлежащие эвакуации.

В целях обеспечения безопасного движения судов по водным артериям города система позволяет выполнять функции по выявлению и фиксации:

– правонарушений и преступлений, совершенных в акватории рек, на мостах и на воде;
– нештатных ситуаций на воде и разводных мостах;
– общего количества судов и плавательных средств, прошедших через контролируемую зону за определенный временной интервал;
– количества судов каждого типа с фиксацией их скорости, габаритов и типа;
– дистанции между судами в период проводки судов;
– превышение скорости движения и нарушения правил судоходства с идентификацией плавательного средства до типа и бортового номера.

Несомненно важными средствами для сбора оперативной информации в период как штатного мониторинга ситуации в городе, так и в период массовых мероприятий в критический период техногенных аварий, природных катаклизмов или террористической угрозы, являются беспилотные летательные аппараты и другие аналогичные взлетно-подъемные средства, способные выполнять мониторинг ситуации на большой территории с использованием самых разнообразных датчиков, сенсоров и средств фото и видеофиксации.

Основными задачами, в частности, решаемыми с помощью БПЛА, являются:

– Мониторинг линейных объектов энергетической инфраструктуры (газопроводов, нефте- и продуктопроводов, ЛЭП)
– Аэрофотосъемочные и сканирующие работы для решения кадастровых задач.
– Обеспечение связи и управления в зоне ликвидации чрезвычайной ситуации или проведения специальной операции.
– Авиационные работы в интересах городских и районных органов власти.
– Авиационные работы в интересах сельхозпроизводителей.
– Геофизические исследования и геологоразведка.
– Правоохранительная деятельность, обеспечение охраны и безопасности.

Таким образом, в качестве наиболее значимых преимуществ внедрения АИС «Безопасный город» можно выделить следующие:

1. АИС «Безопасный город» позволяет выполнять комплексный мониторинг и анализ обстановки в городе, поддержку принятия управленческих решений, а также моделировать

(прогнозировать) и отображать ситуации в едином геоинформационном пространстве в реальном времени в выбранных направлениях с целью оперативного управления по обеспечению безопасности жизнедеятельности города.

2. АИС «Безопасный город» обеспечивает реализацию масштабируемого решения – предоставляет возможность расширения функциональности и оперативного наращивания новых направлений без модификации ядра системы.

3. С помощью средств АИС «Безопасный город» решаются ключевые задачи обеспечения безопасности на объектах повышенного внимания, включая области, лежащие за пределами человеческих возможностей:

– Обработка информации от большого количества видеокамер в едином геоинформационном пространстве с идентификацией и анализом ситуаций, требующих оперативного вмешательства.

– Получение и отображение видеоданных от малых беспилотных летательных аппаратов в реальном времени на трехмерной электронной карте города.

– Удаленная работа через Web-клиент и локальную сеть с подсистемами ГИС 3D в едином информационном пространстве в реальном времени.

– Возможность интеграции решения с различными типами датчиков: видео, аудио, радиолокационных, гидро- и метеорологических, местоположения мобильных объектов, химических, биологических и радиоактивных.

– Моделирование развития ситуаций по направлениям в геоинформационном пространстве и обеспечение взаимодействия между государственными службами.

– Анализ финансовых рисков и экономических угроз.

Внедрение АИС «Безопасный город» позволит:

– Обеспечить повышение безопасности жизнедеятельности за счет решения задач мониторинга и предупреждения угроз.

– Обеспечить эффективное управление масштабными событиями и чрезвычайными ситуациями.

– Обеспечить значительное сокращение времени на принятие решений по управлению кризисными ситуациями.

– Существенно сократить затраты на обеспечение безопасности жизнедеятельности города.

– Оптимизировать организацию взаимодействия экстренных оперативных служб и повысить эффективности их реагирования на возникающие угрозы и вызовы населения.

– Снизить преступность и повысить скорость раскрытия преступлений .

Вместе с тем АИС «Безопасный город» представляет собой только одну из ИС, создаваемых в интересах повышения эффективности управления городским хозяйством. Так как процесс информатизации различных сфер жизнедеятельности города носил до настоящего времени не системный характер (различные ИС разрабатывались исходя из, зачастую, различных представлений о структуре, сопрягаемости и функциональности этих систем), в настоящее время созрела насущная необходимость разработки концепции построения и принципов создания единой межведомственной интегральной автоматизированной ИС (МИАИС) «Интеллектуальный город», способной объединить собой все созданные до настоящего времени в интересах города АИС, обеспечив их совместное функционирование и возможность создания на их основе новых ИС (Рис. 6.).

Архитектура МИАИС «Интеллектуальный город» должна строиться по системным принципам, на подобие АИС «Безопасный город», объединяя последнюю со всем набором ИС города, и должна включать в свой состав:

– РЦОД, обеспечивающий защищенное хранение данных в интересах всех ИС, интегрируемых в рамках МИАИС, и универсальный функциональный санкционированный доступ к этим данным, а также кластеры вычислительных ресурсов для обработки хранимых данных, в интересах всех интегрируемых ИС;

– набор интегрируемых в рамках МИАИС ИС, создаваемых в интересах автоматизации всех сфер жизнедеятельности города;

– единую защищенную телекоммуникационную инфраструктуру для обеспечения взаимодействия всех ОГВ города и функционального санкционированного доступа к данным, хранимым и обрабатываемым в РЦОД,

– сети сенсоров для сбора оперативной и актуальной информации в интересах всех ИС МИАИС;

– городскую ГИС, опирающуюся на данные спутниковых систем и обеспечивающую единую геотопоподоснову визуализации информации в интересах всех ИС,

– набор функциональных интерфейсов, обеспечивающих единообразный универсальный унифицированный доступ как к данным, хранящимся в РЦОД, со стороны ИС, так и к информации о состоянии городского хозяйства и результатах формируемых запросов со стороны широкого круга пользователей системы (государственных служащих, чиновников, населения),

– единый ситуационный центр и центр мониторинга ЧС.

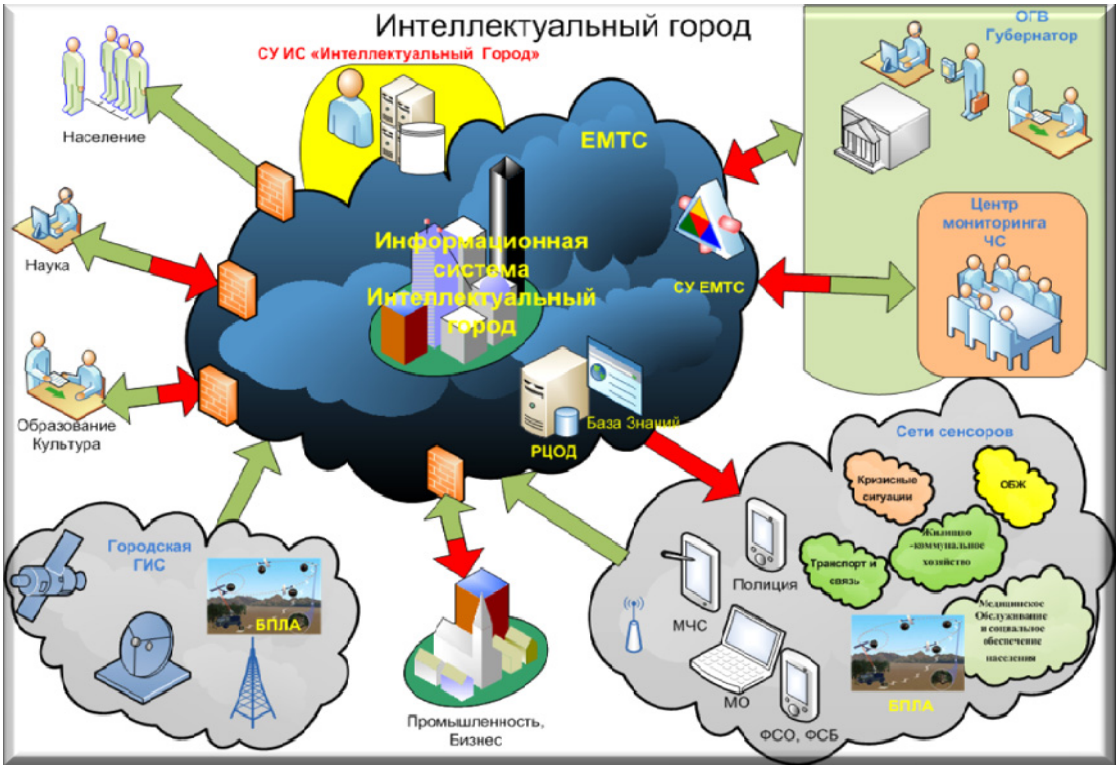


Рис. 6. Межведомственная интегральная АИС «Интеллектуальный город»

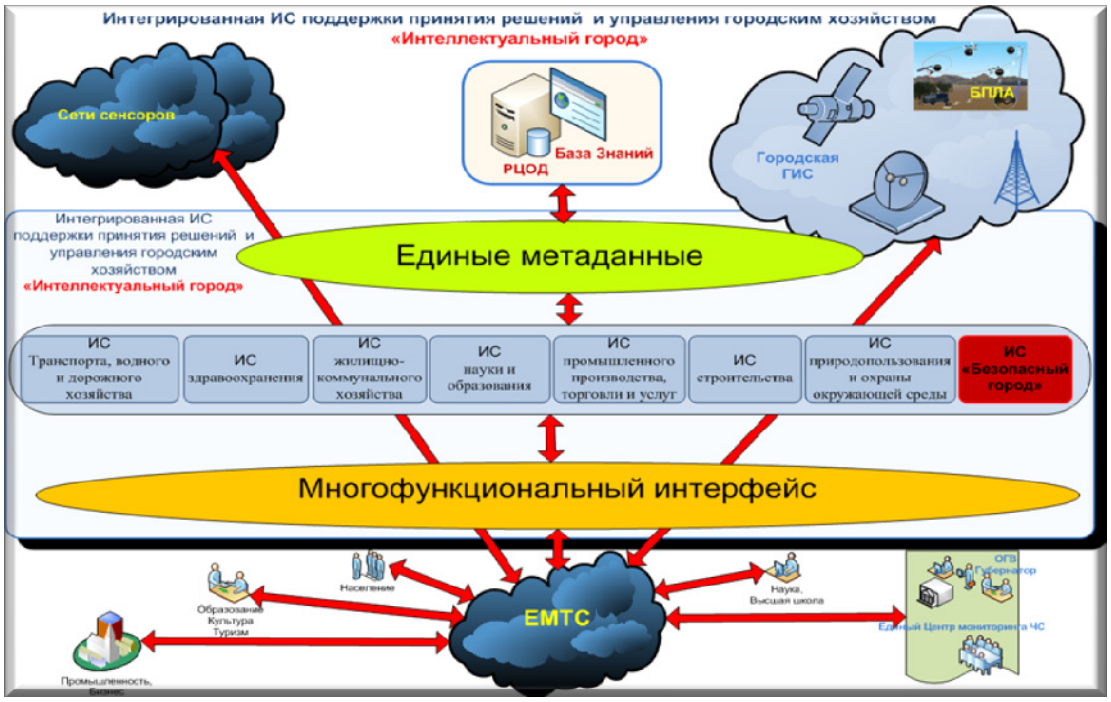


Рис. 7. Архитектура МИАИС «Интеллектуальный город»

Ключевой технологической составляющей МИАИС «Интеллектуальный город» должен стать РЦОД, основными функциональными компонентами которого являются (Рис. 8):

– Хранилище данных емкостью сотни Тбайт с возможностью наращивания емкости до десятков Пбайт информации.

– Кластеризованый вычислительный ресурс повышенной производительности с расширяемой структурой кластера.

– Защищенное телекоммуникационное ядро системы с высокоскоростной шиной Fiber Chanel.

– Система информационной безопасности и балансировки нагрузки.

– Вычислительные ресурсы публичных сервисов МИАИС (WEB-портал).

Для обеспечения выполнения требований по надежности, живучести и оперативности управления в рамках МИАИС «Интеллектуальный город», а также для резервирования ресурсов

хранения и вычислительных ресурсов системы, в целях защиты аппаратно-программных средств системы и данных хранения в аварийных ситуациях необходимо:

– Обеспечение 100% резервирования данных, аппаратных средств хранения данных, вычислительных ресурсов и средств телекоммуникационной инфраструктуры основного РЦОД локальными средствами комплексирования.

– 100% зеркализация данных, аппаратных средств хранения данных, вычислительных ресурсов и средств телекоммуникационной инфраструктуры на базе технических средств резервного ЦОД, с обеспечением репликаций данных в реальном времени, использованием вычислительных ресурсов резервного ЦОД для решения информационных задач, а также обеспечением удаленного доступа пользователей к данным.

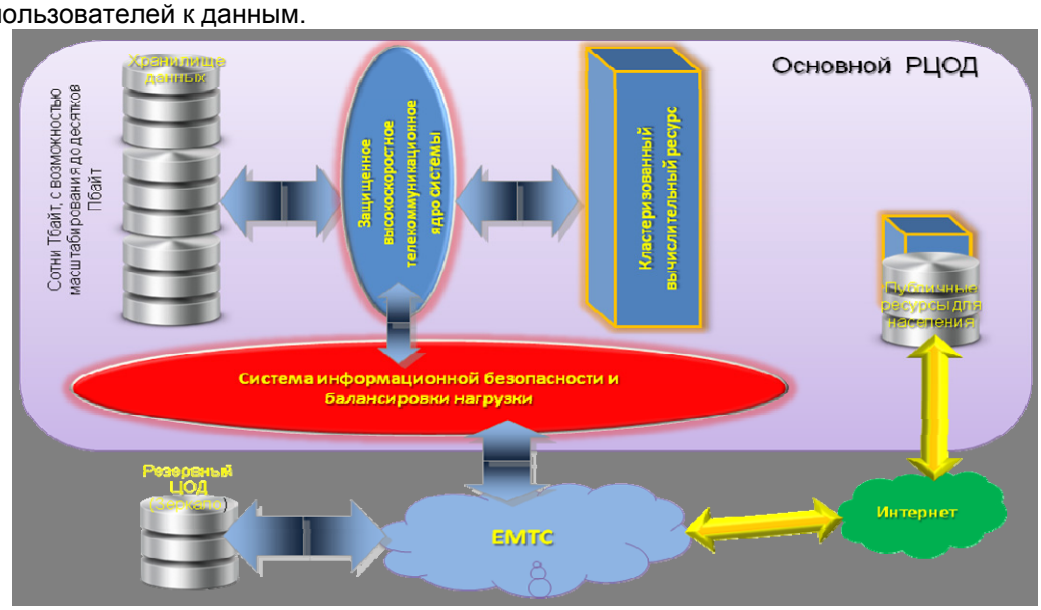


Рис. 8. Функциональная структура ЦОД МИАИС «Интеллектуальный город»

Учитывая современное состояние развития средств информационной поддержки в городе в рамках уже созданных ИС можно рассмотреть следующие этапы создания МИАИС «Интеллектуальный город»:

1 Этап. Создание основных функциональных компонент – технологической и информационной составляющих МИАИС «Интеллектуальный город»:

– развитие ЕМТС, создание РЦОД, развертывание сети сенсоров и модернизация аппаратных средств оконечных пользователей (техническое переоснащение ОГВ);

– разработка архитектуры АИС, разработка структуры единых метаданных и единых интерфейсов доступа, разработка и модернизация профильных ИС с поддержкой стандартных интерфейсов.

2 Этап. Создание пилотной зоны МИАИС «Интеллектуальный город» и ее эволюционное функциональное наполнение. Опытная эксплуатация ИС.

3 Этап. Переход к полнофункциональной МИАИС «Интеллектуальный город» и ее модернизация (развитие).

УДК 347.77

ИНФОРМАТИЗАЦИЯ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

Кононов Олег Александрович[1], Кононова Ольга Васильевна[1], Попенко Николай Васильевич[2],
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д. 67,
[2]Президиум Российской Академии Наук,
Россия, Москва, Ленинский проспект, дом 32 А,
e-mails: o2kon@mail.ru, nik-popenko@yandex.ru

Аннотация: В статье рассмотрены вопросы организации правового обеспечения в условиях становления информационного общества.

Ключевые слова: *информатизация, информационные технологии, правовое обеспечение, информационная безопасность.*

INFORMATIZATION AND LEGAL SUPPORT

Oleg Kononov[1], Olga Kononova[1], Nikolai Popenko[2],
[1.]Saint-Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya street 67,
[2.]Presidium of the Russian Academy of Sciences,
Russia, Moscow, Leninsky Prospekt 32A,
e-mails: o2kon@mail.ru, nik-popenko@yandex.ru

Abstract: The article describes the organization of legal support in the information society environment.

Keywords: *informatization, information technology, legal support, information security.*

Введение. На сегодня очевидным является тот факт, что основной чертой современного общества является переход от индустриальной экономики к экономике, базирующейся на знаниях, к информационному обществу [1].

Преобладающим направлением становится создание средств обработки информации, информационных услуг и информационных технологий. Широкая информатизация общества приводит к возникновению совершенно новых отношений в правовом поле. Так, например, использование современных коммуникационных связей привело к необходимости создания дополнительных структур, и в частности, удостоверяющего центра для регистрации сертификата ключа цифровой подписи.

Объективно появилась необходимость комплексного изучения правовых, организационных, технических, социологических (и даже медицинских) вопросов, позволяющая получить необходимые знания для корректного использования преимуществ новых информационных технологий. Возникающие между правовыми субъектами информационные отношения, построенные на использовании цифровых форм представления данных, обмене, преобразовании, распространении информации должны сочетаться с возможностями, прежде всего, правовой защиты.

Правовые проблемы. Правовые проблемы возникают в связи с превращением информации в основной стратегический ресурс развития общества, необходимостью правовой регламентации производства, обработки и использования этого ресурса.

Эти проблемы включают в себя [2]:

– общие проблемы правового регулирования в инфосфере, в том числе правовая охрана программных средств, правовое регулирование договорных отношений, экономический и правовой режим информационных ресурсов, интеллектуальной собственности;

– проблемы правонарушений в инфосфере, к которым относятся имущественная ответственность в последней, применение новых информационных средств и технологий и доказательное право, компьютерные преступления;

– проблемы развития инфосферы в области права, в которые входят применение экспертных систем в этой области, криминалистическое моделирование преступной деятельности, компьютерная подготовка юристов и повышение их информационной культуры.

Отсутствие действенного организационно-правового механизма информатизации является в настоящее время одним из факторов, сдерживающих процесс информатизации, как на государственном, так и на региональном уровнях.

Развитое организационно-правовое обеспечение должно [2]:

– оперативно выявлять и задавать приоритеты информатизации, определяющие статус ее программы в регионе, статус каждой из ее подпрограмм, мероприятий и работ, а также уровень льгот в системе кредитования и налогообложения;

– обеспечивать на основе международных и государственных правовых норм доступ пользователей к базам данных и знаний, а также защиту баз от несанкционированного доступа;

– гарантировать право предприятий (организаций) и граждан от распространения и использования информации об их деятельности и жизни, имеющей личный или конфиденциальный характер;

– регламентировать порядок передачи предприятиями (организациями) и частными лицами данных и знаний соответствующим предприятиям (организациям) для создания баз данных и баз знаний и определять авторские и другие права сторон;

– регулировать статус запросов в базы данных и определять приоритеты их обслуживания;

– регламентировать обязательства предприятий (организаций) по предоставлению информации в соответствующие международные базы данных;

– обеспечивать защиту прав разработчиков продуктов интеллектуального труда в сфере информатизации.

Формирование эффективного организационно-правового механизма информатизации включает в себя:

– определение отношений собственности в области информатики и информатизации;

– разработку принципов и методов формирования информационных ресурсов территории;

– разработку организационных, правовых и экономических механизмов информационного взаимодействия субъектов территории с различными формами собственности;

– разработку требований к системе обеспечения информационной безопасности.

Правовое обеспечение информатизации предусматривает:

– законодательное закрепление прав граждан, организаций, государства на свободный поиск, получение, использование и распространение информации, а также гарантию реализации этого права за исключением случаев, установленных законодательством;

– установление правового режима информации;

– обеспечение доступности информации, не отнесенной в установленном законом порядке к данным с ограниченным доступом;

– установление правовых форм защиты информации и гарантий информационной безопасности;

– правовую защиту авторских и иных прав в области информационных отношений.

На рисунке 1 представлены элементы правоотношений в инфосфере, показаны права юридических и физических лиц с указанием областей ограничения при информационных взаимодействиях, имеющие место при этом обязанности, а также ответственность, возникающие при нарушении или неправомочном построении этих взаимодействий [1].

Информационная безопасность. При информационном взаимодействии, как отправитель информации, так и ее получатель не должны представлять друг для друга информационную угрозу. Поскольку при информационном взаимодействии передается информация, то существенное значение имеет то, как эта информация передается, т.е. каким образом осуществляется коммуникация между объектами. Поэтому коммуникации и называют связующими процессами. Коммуникация и информация различные, но связанные между собой понятия. Коммуникация включает и то, что передается, и то, как это передается.

Для обеспечения информационной безопасности передаваемой в системе информации, для каждого элемента коммуникации должны быть предусмотрены средства (методы) защиты.

Цель защиты информации – обеспечить ее конфиденциальность и устойчивость к интеллектуальным «диверсионным» воздействиям при ее передаче, обработке и хранении.

При этом информацию защищают по следующим основным направлениям:

– предотвращение перехвата через электромагнитные излучения и звуковые волны;

– контроль и управление доступом;

– защита от программ-вирусов;

– защита от несанкционированного декодирования (расшифровки) информации;

– предотвращение хищения или уничтожения носителей, разрушения и вывода из строя информационных средств и механизмов защиты.

К основным принципам защиты информации относятся:

– органичное встраивание мероприятий по мере информатизации по защите информации;

– рациональное сочетание централизованных и региональных (местных) мероприятий по защите информации;

– многоуровневая организация защиты информации;

– избирательность и экономическая целесообразность (достаточность);

– непрерывность и гибкость;

– совместимость и стандартизация способов и средств защиты информации и информационных технологий.

В зависимости от числа уровней и степени сложности объектами информационной защиты являются:

– речь, тексты документов и другие виды информации на различных материальных носителях;

– телефонные, телеграфные аппараты, проводные линии связи;

– средства оргтехники, аудио- и видеотехника;

– персональные компьютеры, универсальные ЭВМ и их программное обеспечение;

– базы данных и знаний, информационно-поисковые системы;

– беспроводные каналы связи, системы передачи данных;

– локальные и интегрированные информационно-вычислительные системы;

– интеллектуальные системы;

– Интернет;

– Грид-системы.

– Грид (англ. Grid – решетка, сеть) – согласованная, открытая и стандартизованная компьютерная среда, которая обеспечивает гибкое, безопасное, скоординированное разделение вычислительных ресурсов и ресурсов хранения информации, которые являются частью этой среды, в рамках одной виртуальной организации.

Рис. 1. Элементы информационных правоотношений

Безопасность информации обеспечивают при помощи законодательно-правовых актов, организационных мероприятий и научно-технических средств, образующих систему ее защиты, причем последние играют существенную роль при использовании информационных технологий.

Законодательно-правовые аспекты защиты информации – прерогатива федеральных законодательных органов власти Российской Федерации. Законодательно-правовая стратегия региона (на местах) должна выражаться в широком участии специалистов и общественности в инициации, обсуждении и подготовке законодательных и нормативных актов.

Вариант целесообразной организационной структуры системы обеспечения информационной безопасности регионального уровня включает в себя:

– координирующий орган на уровне руководства регионом;

– отдел информационной безопасности департамента связи и информатизации;

– региональные специальные центры федеральных органов власти по отдельным направлениям защиты информации;

– региональный координационно-внедренческий центр, головную научно-исследовательскую организацию;

– службы обеспечения безопасности информации в объединениях, предприятиях, банках, организациях и т.д.;

– вузы и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации.

Научно-технические аспекты защиты информации связаны с развитием высоконадежных аппаратных и аппаратно-программных методов и средств. Их роль в решении проблем защиты информации весьма значительна, что следует учитывать при проведении мероприятий по обеспечению безопасности информации.

Глобализация открытых компьютерных и телекоммуникационных сетей, быстрый рост мирового рынка информационных технологий, продуктов и услуг, формирование международного информационного пространства создают предпосылки для нарушения традиционных механизмов обеспечения геополитической целостности государств, оказывают серьезное воздействие на многие элементы государственности и национальных правовых систем. Растет осознание значения международно-правовых механизмов, повышается роль нравственной компоненты в регулировании информационных отношений в обществе.

Нормативно-правовой базис. Нормативно-правовой базис информационной политики, как и политики вообще, составляет совокупность норм права и механизмы их реализации, которые определяют, в первую очередь, права граждан, юридических лиц и государства на свободное получение, распространение и использование информации, защиту информации и интеллектуальной собственности.

При формировании такого базиса следует учитывать все особенности отношений, складывающихся между субъектами при информатизации и использовании информационных и телекоммуникационных технологий и информационных ресурсов. Эти особенности новы для института права и влияют практически на все аспекты информационных отношений, которые все глубже проникают во все сферы общественной жизни.

К данным особенностям относится следующее [3]:

– информация обменивается в электронной цифровой форме, что в сочетании с возможной легкостью и оперативностью ее создания, распространения, модификации или уничтожения определяет проблему обеспечения доказательств и соответственно создает условия объективного усложнения защиты прав и интересов лиц;

– создание и развитие информационных ресурсов и систем в Интернете и иных сетях электросвязи, а также распространение информации в этих сетях происходит исключительно в рамках принятых технических стандартов и протоколов, что определяет высокую значимость технических норм для характера отношений и их регулирования;

– существующий уровень технологий обмена информацией позволяет осуществлять его в режиме реального времени (без заметной временной задержки для субъектов отношений);

– субъекты отношений распределены в пространстве, в связи с чем возникает проблема определения юрисдикции регулирования отношений со стороны различных государств и административно-территориальных образований:

– в качестве субъектов информационных отношений выступают лица, распространяющие и потребляющие ту или иную информацию, и лица, владеющие средствами распространения этой информации и являющиеся информационными посредниками (провайдерами – англ. provider – поставщиками услуг Интернета), подключающими пользователей к сети через свои компьютеры;

– широкие возможности и востребованность механизмов саморегулирования, при которых собственники и владельцы информационных ресурсов (провайдеры) могут регулировать и контролировать обмен информацией;

– высокие технические, образовательные, культурные требования к субъектам информационных отношений и одновременно излишняя вера в возможности информационных и телекоммуникационных технологий и в безопасность отношений, возникающих при их использовании.

Информационное право. В силу относительной новизны и высокой социальной роли информационных отношений, а также особенностей существующей системы права, в России эти отношения регулируют в рамках различных отраслей права:

– конституционного (право на информацию);
– гражданского (электронные сделки и расчеты);
– административного (законодательство о связи, информационная безопасность).

Этим порождается несбалансированная система юридических дефиниций, различные подходы к субъективному делению лиц, участвующих в информационных процессах и соответственно сосуществование различных способов определения прав и обязанностей субъектов информационных отношений. Такое положение вызывает необходимость в существовании самостоятельной комплексной отрасли права – информационного права.

Действующие федеральные законы «Об информации, информационных технологиях и о защите информации», «О связи», «О государственной тайне», «О рекламе», «О средствах массовой информации» и другие заложили основы законодательного регулирования информационных отношений в России с учетом мировой практики, современного развития информационных технологий и обеспечения информационных прав субъектов правоотношений. Эти законы являются базовыми при формировании и применении информационного права в регионах России. Однако состав и качество этих законов позволяет говорить лишь о начале формирования отрасли информационного права в России и его неравномерном и несбалансированном развитии [4], [5].

Региональная информационная политика. Представляется целесообразным к основным принципам региональной информационной политики в сфере правового регулирования информационного взаимодействия отнести [6]:

– безусловное правовое равенство всех участников информационного взаимодействия вне зависимости от их политического, социального и экономического статуса; гарантированность прав граждан и юридических лиц в инфосфере;

– формирование и развитие информационного права в регионе с учетом федерального законодательства и в пределах прерогатив органов власти региона;

– ограничение доступа к информации в регионе только на основе соответствующего законодательства и, как исключение, из общего принципа открытости информации;

– персонификация ответственности за сохранность информации, ее засекречивание и рассекречивание;

– правовая защита населения региона от ложной, искаженной и недостоверной информации, поступающей через СМИ и другие каналы;

– предоставление населению региона необходимых информационных услуг, правовое обеспечение возможности доступа к мировым информационным ресурсам и глобальным информационным сетям;

– совместимость информационного права в регионе с российским и мировым информационным правом.

Заключение. Реализация такой информационной политики в сфере информационного права позволит создать необходимые условия для реализации прав граждан и юридических лиц в инфосфере, развития и повышения конкурентоспособности отечественного сектора информационных и телекоммуникационных технологий, повысить эффективность системы государственного управления за счет оптимизации информационных процессов в государственных органах.

СПИСОК ЛИТЕРАТУРЫ

1. Юсупов Р.М., Заболотский В.П. Концептуальные и научно-методологические основы информатизации //СПб.: Наука, 2009. – 542 с.
2. Кононов О.А., Кононова О.В., Попенко Н.В. Об организационно-информационном обеспечении информатизации. XIV Санкт-Петербургская международная конференция «Региональная информатика – 2014 (РИ–2014)»: материалы конференции. – СПб.: СПОИСУ, 2014. С.179–180.
3. Кононов О.А., Кононова О.В., Попенко Н.В. Информатизация и информационное право. XIV Санкт-Петербургская международная конференция «Региональная информатика – 2014 (РИ–2014)»: материалы конференции. – СПб.: СПОИСУ, 2014. С.178–179.
4. Кононов О.А., Кононова О.В. Социальные и этические аспекты информационной безопасности в корпоративной среде // Проблемы информационной безопасности. Компьютерные системы. Научный журнал СПбГПУ. СПб.: изд-во Политехнического университета, 2009, № 4. С.72–77.
5. Кононов О.А., Кононова О.В. Социальные и этические аспекты обеспечения информационной безопасности // Проблемы управления (научно-технический журнал ИПУ РАН). М: ИПУ РАН, 2009. № 1.С. 76–80.
6. Путилин А.Б., Попенко Н.В. Правовое обеспечение информационных технологий. М.: Изд-во МГОУ, 2011. 286 с.

УДК 004.056:61

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ЭФФЕКТИВНЫЙ МЕТОД ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД

Парфенов Николай Петрович,
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1,
e-mail: parfenov-nikolai@mail.ru.

Аннотация: В статье рассмотрены основные методы защиты персональных данных сотрудников ОВД в служебной деятельности.

Ключевые слова: *персональные данные; защита персональных данных; обезличивание персональных данных; система защиты информации; организационные меры (методы) защиты информации.*

DEPERSONALIZATION OF PERSONAL INFORMATION – AN EFFECTIVE METHOD OF PROTECTION OF PERSONAL INFORMATION OF STAFF OF DEPARTMENT OF INTERNAL AFFAIRS

Nikolay Parfenov,
The Ministry of Internal Affairs St. Petersburg University (At the Ministry of Internal Affairs of Russia),
Russia, St. Petersburg, Letchika Pilyutova str. 1,
e-mail: parfenov-nikolai@mail.ru.

Abstract: The main methods of protection of personal information of staff of Department of Internal Affairs in office activity are considered.

Keywords: *personal information, protection of personal information, depersonalization of personal information, information security system, organizational measures (methods) of information security.*

Введение. На современном этапе развития общества защита информации приобретает актуальное значение.

Наиболее важной задачей в МВД России является обеспечение защиты информации различных уровней конфиденциальности (секретности), а также информации, содержащей сведения ограниченного распространения (служебной, банковской, персональных данных). Основным звеном в системе защиты информации предприятия, организации становится технология защиты персональных данных его работников. На данный момент времени ужесточены нормы

законодательства по защите персональных данных работников. В связи с этим необходимо позаботиться о соблюдении установленных в этой сфере требований. В целях дополнительной защиты сведений о гражданах в Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ [1] были внесены существенные поправки, вступившие в силу с 1 июля 2011 года (см. Федеральный закон от 25 июля 2011 г. № 261-ФЗ) [2]. Изменилось само понятие персональных данных, под которыми теперь понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (п. 1 ст. 3 закона № 152-ФЗ).

Сотрудники ОВД также являются субъектами персональных данных, согласно той же статье 3 Федерального Закона «О персональных данных».

Необходимо отметить, что согласно Федеральному закону «О службе в органах внутренних дел Российской Федерации» от 30.11.2011 № 342-ФЗ для сотрудников внутренних дел отдельно прописана защита их персональных данных, что означает дополнительное предоставление гарантий при защите их персональных данных:

– обработка персональных данных проводится для соблюдения требований Конституции Российской Федерации, настоящего Федерального закона и других нормативных правовых актов;

– защита персональных данных сотрудников МВД от неправомерного применения или утраты, осуществляется средствами федерального органа исполнительной власти в сфере внутренних дел в соответствии с требованиями настоящего Федерального закона и других нормативных правовых актов.

В подразделениях ОВД проходят службу сотрудники, которые имеют различные формы допуска к конфиденциальной информации. В связи с этим, для обеспечения требований по защите и допуску различных групп к информации разной степени секретности предварительно разделяют объекты информатизации по важности и присваивают категории. Категории определяются конфиденциальностью информации, обрабатываемой на соответствующем объекте информатизации. При этом для каждой категории определяется соответствующий набор требований по ее защите. После присвоения объекту информатизации соответствующей категории специальная комиссия проводит комплекс режимных и технических мероприятий. Результатом данных мероприятий является разработка аттестата соответствия, в котором указывается, что объект информатизации соответствует требованиям стандартов и нормативных документов по технической защите информации.

Защита персональных данных сотрудников полиции имеет свои специфические особенности, и этому обстоятельству мне бы хотелось уделить особое внимание. В основном, специфические особенности защиты персональных данных обусловлены условиями прохождения службы сотрудниками правоохранительных органов и вытекают из положений нижеперечисленных основных нормативных правовых документов:

– Конституция РФ (Статьи 23, 24);
– Трудовой кодекс РФ (Глава 14);
– Федеральный закон «О полиции»;
– Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006г.;
– Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства Российской Федерации № 781 от 17 ноября 2007 г.;
– «Порядок проведения классификации информационных систем персональных данных», утвержден приказом ФСТЭК России, ФСБ России Мининформсвязи России № 55/86/20 от 13 февраля 2008 г.

Персональные данные – в общепринятом смысле термина, это – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Как правило, идентификация личности проводится по сведениям, содержащимся в паспорте. Кроме этого, идентифицировать личность позволяют и дактилоскопические данные.

Для сотрудников правоохранительных органов, предназначенных для борьбы с преступностью, эти данные имеют непосредственное значение.

В связи с этим 25 июля 1998 года был принят Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации».

Также приняли инструкции, регулирующие алгоритм проведения дактилоскопической регистрации для определенных категорий лиц гражданской государственной службы.

Например, для сотрудников органов внутренних дел и спасателей аварийно-спасательных служб обязательна дактилоскопическая регистрация. Также утверждена Инструкция о процедуре проведения обязательной государственной дактилоскопической регистрации работников органов по контролю над оборотом наркотических средств и психотропных веществ согласно приказа № 18 от 28 января 2004 г. Государственного комитета РФ по контролю над оборотом наркотических средств и психотропных веществ.

Данные сведения необходимы работодателю, чтобы заключить трудовой договор, заполнить личную карточку № Т2, помочь работнику в обучении, продвижении по службе, обеспечить его личную безопасность, контролировать количество и качество выполняемой им работы.

Персональные данные относятся к конфиденциальной информации, то есть, к которой нет свободного доступа. В настоящее время защита информации на предприятиях, в организациях, органах

внутренних дел приобретает актуальное значение. Ключевое место в технологии защиты персональных данных работников занимает разработка положения. Положение о защите персональных данных работника – это основной документ, регламентирующий алгоритм защиты персональных данных работника на конкретном предприятии. Данный документ занимает основное место в системе защиты информации предприятия. Как правило, положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работника, а также ведения его личного дела в соответствии с трудовым законодательством Российской Федерации [3]. Положение о защите персональных данных работника - это внутренний (локальный) документ предприятия. Данный документ разрабатывает кадровая служба предприятия. На сегодняшний день закон не установил строгой формы этого документа, но он должен соответствовать требованиям, которые предъявляет к защите персональных данных работника Трудовой кодекс РФ.

Предприятие или организация, обрабатывающая такие данные, по своему статусу соответствует понятию оператора. Уточнены принципы обработки сведений (ст. 5 закона № 152-ФЗ). В законе № 152-ФЗ появилась новая статья 18.1. В ней предусмотрены меры, направленные на обеспечение обновленных требований. Работодатель разрабатывает перечень мер, необходимых для выполнения обязанностей по обработке персональных данных. Обращаем особое внимание: предприятию или организации теперь помимо Положения по защите персональных данных работников, которое принималось в соответствии с Трудовым кодексом РФ, необходимо разработать новый документ – Политику в отношении обработки персональных данных [4, с. 16–18].

В развитие вопросов указанного направления издан Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (Зарегистрировано в Минюсте России 10 сентября 2013 г. № 23395) [5].

Согласно статьи 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без применения дополнительной информации установить принадлежность персональных данных конкретному носителю персональных данных.

Далее в статье более подробно рассмотрим свойства, методы обезличивания персональных данных и проведем их оценку.

Обезличивание персональных данных необходимо не только для их защиты от несанкционированного использования, но и для дальнейшей обработки. Поэтому обезличенные данные должны сохранять основные характеристики обезличиваемых персональных данных. Далее назовем основные свойства обезличенных данных:

– полнота – это сохранение информации в полном объеме о конкретных носителях персональных данных, которая имелась до обезличиваня;

– структурированность – это сохранение структуры обезличенных данных конкретных носителей, имевшейся до обезличивания;

– семантическая целостность – это сохранение семантики персональных данных конкретных субъектов в процессе их обезличивания;

– анонимность – это неспособность однозначной идентификации носителей персональных данных, полученных в процессе обезличивания, без использования дополнительной информации.

Наиболее практичными считаются следующие методы обезличивания:

– метод введения идентификаторов – это замена персональных данных идентификаторами, путем создания каталогов соответствия идентификаторов исходным персональным данным;

– метод изменения состава или семантики – это изменение состава или семантики персональных данных конкретных субъектов методом замены их результатами статистической обработки, объединения или исключения части сведений;

– метод декомпозиции – это разделение множества персональных данных конкретных субъектов на подмножества с дальнейшим обособленным хранением их;

– метод перемешивания – это перемещение и перестановка отдельных записей в множестве персональных данных конкретных субъектов.

Необходимо подчеркнуть и отметить, что методы обезличивания данных постоянно развиваются, совершенствуются.

Заключение. Подводя итоги рассмотренных вопросов, необходимо отметить, что применение рассмотренных в статье методов обезличивания данных позволит повысить качество обработки персональных данных и обеспечит более высокую степень защиты персональных данных сотрудников ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
2. Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных».
3. Трудовой Кодекс Российской Федерации (ТК РФ) № 197-ФЗ от 30.12.2001 г.
4. Егорова И.С. Работа с персональными данными: новые правила. Журнал «Учет в строительстве» № 12, 2011 г. – С.16–18.
5. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (Зарегистрировано в Минюсте России 10.09.2013 № 29935).

УДК 343.34

ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Шалагинова Ольга Борисовна,
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1,
e-mail: shans331@yandex.ru

Аннотация: В статье рассмотрены основные приоритеты вспомогательных задач обеспечения безопасности информационной сферы. Информационная сфера это общество, организации, компании. Безопасность информации в компьютерных системах включает обеспечение трех основополагающих компонент: конфиденциальности, целостности, доступности. В настоящее время главный акцент ставится на компьютерную защищенность в деятельности Органов внутренних дел.

Ключевые слова: *информация; безопасность; компьютеризация; секретность; целостность.*

TECHNOLOGY OF INFORMATION SECURITY IN LAW ENFORCEMENT

Shalaginova Olga Borisovna,
The Ministry of Internal Affairs St. Petersburg University (At the Ministry of Internal Affairs of Russia),
Russia, St. Petersburg, Letchika Pilyutova str. 1,
e-mail: shans331@yandex.ru

Abstract: The article describes the main priorities of the subsidiary objectives of ensuring security of the information sphere. The information field is a society, organization, company. Information security in computer systems includes the provision of three basic components: confidentiality, integrity, availability. Currently the main emphasis is on computer security in the activities of internal Affairs Bodies.

Keywords: *information; safety; computerization; privacy; integrity.*

Введение. Необходимость обеспечения информационной безопасности всегда была актуальной. С развитием прогресса и массовой компьютеризации существенно возросла роль защиты информации. Так как правоохранительные структуры обрабатывают большие потоки информации, которая в настоящее время автоматизирована, в системе Министерства внутренних дел безопасности информационных данных уделяют особое внимание. Современная инфраструктура и инструментарий жизнедеятельности и коммуникаций в современных информационных технологиях изменили и обострили проблему безопасности информации. Вспомогательные задачи обеспечения информационной безопасности перешли в основные приоритеты, так как возросла возможность несанкционированного доступа к информации, несанкционированного получения информации, а также возможность мгновенного разрушения информационных ресурсов.

Компьютерная безопасность – это термин, представленный одним из компонентов наиболее широкого понятия «информационная защищенность», которое означает уровень безопасности информационной сферы (общество, организации, компании) от всех опасностей (внутренних и наружных). Основными эпизодами в понятии «информационная защищенность» считаются: информационная сфера (объект), опасности (внутренние и внешние), состояние безопасности (предмет объекта). В этом рассмотрении широта понятия «компьютерная защищенность».

Понятие «сохранность информации» включает три основополагающих компонента:

– конфиденциальность (секретность);
– целостность (неделимость);
– доступность.

В этом варианте, секретность информации – специфичное свойство отдельных видов, категорий информации, необъективно устанавливаемое ее владельцем, как скоро быть может причинен вред от ознакомления с материалами неуполномоченных на то лиц, к примеру: случается утечка данных по вибро-акустическому каналу утечки данных.

Целостность данных можно толковать как неискаженность, полноту, правдивость, адекватность информации, то есть то ее качество, при котором текстура и содержание данных имеют все шансы быть отнесены и изменены только лишь уполномоченными лицами и процессами. Следовательно, обеспечение охраны данных в системе компьютера значит точь-в-точь такую технологию работы с этими данными, при которой сведения подлежат изменению, модифицируются исключительно уполномоченными лицами и в действиях их передачи и хранения исправляются ошибки. Например: деятельность информационных центров Министерства внутренних дел.

И, в конце концов, под правомерной доступностью данных (информации) понимается признак информации, при котором преграды доступа к сведениям и закономерному ее применению владельцем либо уполномоченными лицами отсутствуют. Вследствие чего же, сохранность материалов в компьютерной системе поддерживается ее сохранностью, возможностью к

возобновлению при сбоях и разрушениях, также без преград работы с ней уполномоченных лиц?

Весомо выделить, фактически только лишь единовременное обеспечение всех трех компонентов (секретности, неразрывности и открытости) которые обеспечивают состояние защищенности данных. Термин «безопасность», как правило, считается тождественным термину «сохранность». В масштабах приведенного выше определения, второй стороной компьютерной защищенности считается сохранность (надежность, безотказность) функций компьютерных систем.

Первая основополагающая определяется безотказностью оборудования (технических средств обработки, сбережения, передачи и представления информации) и безотказностью программного обеспечения (недоступность перебоев в работе программ).

Вторая основополагающая – равнозначность функций. Определяется тем, что программное обеспечение характеризуется неделимостью программно-аппаратной конфигурации системы компьютера (состава программного обеспечения, индивидуальных настроек, программ и особенностей).

При всем этом надлежит отметить, что две данные основополагающие компьютерной защищенности считаются взаимозависимыми. Например, при несоблюдении безопасности информации в компьютерной системе (несоблюдении конфиденциальности, монолитности и/или доступности данных) почти всегда не поддерживается многофункциональная сохранность компьютерной системы. В противном случае, основополагающие компоненты компьютерной защищенности не будут являться взаимосвязанными. Сведения в приборе персональный компьютер имеют возможность находиться в безопасном состоянии, учитывая их секретность, сохранность и неделимость, хотя в результате сбоев оборудования или программного обеспечения, нарушения целостности программного обеспечения или полноты программно-аппаратного вида, функции компьютерной системы не будут выполняться. Кроме того существенно важно, что вследствие отличительных черт ситуации развития электронно-вычислительной техники, две основополагающие компьютерной сохранности рассматривались и развивались в предопределенной степени самостоятельно, причем, даже не говоря уже о том, что вторая основополагающая, непосредственно сохранность функций, рассматривалась исходя из убеждений обеспечения надежности вычислительной техники (оборудования и программного обеспечения).

Заключение. Как следует из этого, и в литературе, и в стереотипах, в настоящее время под компьютерной защищенностью в деятельности Органов внутренних дел понимается, в первую очередь (и в основном), первая ее составляющая, т.е. безопасность информации в компьютерных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Гасумова С.Е. Информационные технологии в социальной сфере. – М.: Дашков и Ко, 2011. – 248 с.
2. Грушо А.А., Применко, Э.А., Тимонина Е.Е.. Теоретические основы компьютерной безопасности: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2009. – 272с.

УДК 004.056

РАЗВИТИЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ И БЕЗОПАСНОСТЬ

Советов Борис Яковлевич[1], Колбанев Михаил Олегович[2], Татарникова Татьяна Михайловна[3]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2,3] Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mails: bysovetov@mail.ru, mokolbanev@mail.ru, tm-tatarn@yandex.ru

Аннотация: Рассматриваются направления развития информационных технологий, в рамках которых технология инфокоммуникации рассматривается как предметная область систем обеспечения безопасности.

Ключевые слова: *информационное взаимодействие; информационная технология; информационное общество; интеллектуальное общество; технология инфокоммуникации; метауровни информационной безопасности.*

TECHNOLOGY INFORMATION COMMUNICATION AND SECURITY

Sovetov Boris[1], Kolbanev Mikhail[2], Tatarnikova Tatiana[3]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2,3] Saint-Petersburg State University of Economics
Russia, St. Petersburg, Sadovaya str., 21,
e-mails: bysovetov@mail.ru, mokolbanev@mail.ru, tm-tatarn@yandex.ru

Abstract: Considers the ways of development of information technologies, in which the Infocommunications technology is considered as a subject area of security systems.

Keywords: *information interaction; information technology; information society; intellectual society; technology infocommunication; meta-level information security.*

Введение. Любую деятельность человека сопровождает информационное взаимодействие. Оно осуществляется на двух метауровнях и требует на каждом из них решения специфических проблем безопасности [1 - 3].

1. Обобщенная модель процесса информационного взаимодействия и безопасности. К ключевым объектам обобщенной модели процесса информационного взаимодействия и безопасности, представленной на рисунке 1, относятся [4]:

– смысл – содержание некоторого высказывания;

– язык – набор знаков и связей между знаками, для которых существуют правила смысловой интерпретации,

– данные – материальная форма представления знаков языка не согласованная (сообщение) или согласованная (сигнал) с физическим пространством.

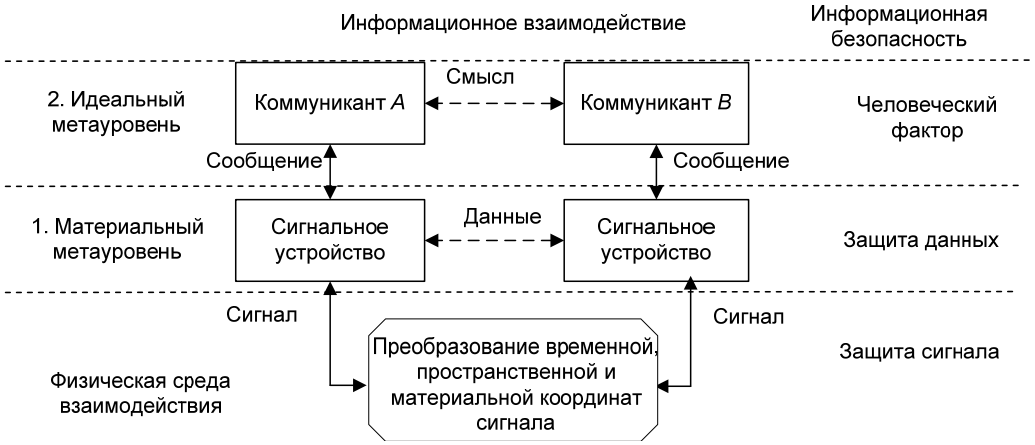


Рис. 1. Обобщенная модель процесса информационного взаимодействия и безопасности

Такая система понятий является обобщением общей схемы системы связи, которая была предназначена К. Шенноном для «точного или приближенного переноса сообщения между двумя точками пространства» [5]. К. Шеннон не учитывал идеальную (смысловую) сторону информационного взаимодействия, так как она «не имеет отношения к технической стороне вопроса».

При построении моделей безопасности нельзя игнорировать идеальный метауровень, который является продуктом человеческого сознания. Информационные процессы зависят здесь от используемых языков взаимодействия и связаны с особенностями мышления людей. На этом метауровне обеспечивается защита смыслов с учетом человеческого фактора. Для этого человек, обладающий секретным знанием, рассматривается как часть системы и одно из уязвимых мест в системе безопасности. Разрабатываются мероприятия, блокирующие такие ошибки людей, которые могут привести к успешным информационным атакам, имеющим цель раскрыть секретные смыслы противнику [2],[4].

На материальном метауровне происходит обмен данными, а соответствующие информационные процессы представляют собой последовательность операций над данными, как материальными объектами. Здесь осуществляется защита логических свойств сообщений и языка информационного взаимодействия, например, математическими методами криптографии путем представления смыслов на языке, который не знает противник (шифрование, цифровая подпись и др.) [3];

Физическая среда взаимодействия расширяет понятие канала связи, которое использовал К. Шеннон. Она преобразует временную, пространственную и физическую координаты существования сигнала, что превращает ее, соответственно, в память, канал связи или процессор. Защита данных здесь обеспечивается на уровне сигнала и физических законов его существования, например, при попытке разрушить или модифицировать память, от побочных излучений, помех или наводок канала связи, при воздействии на сигналы, обрабатываемые процессором, программным путем и др. [2].

2. Направления развития технологий информационного взаимодействия. Предлагаемая модель позволяет выделить два направления развития технологий информационного взаимодействия – экстенсивный и интенсивный (рисунок 2). Цель экстенсивного развития заключается в увеличении объемных характеристик информационных систем путем создания инфокоммуникационных сетей и систем. Принцип интенсивного развития предполагает создание интеллектуальных информационных систем. Для этого необходимо организовать данные в сложные структуры при помощи связей, прописанных в метаданных, и разработать инструменты, позволяющие

автоматизировать процесс создания новых или перенастройки уже созданных технологий с учетом изменяющихся потребностей [6],[7].

Рис. 2. Направления развития информационных технологий

Движение в первом направлении, в основном, связано с совершенствованием информационных технологий физической среды взаимодействия и материального метауровня, в то время как второе направление предполагает появление на идеальном метауровне наряду с человеком и интеллектуальных систем. Соответственно этому экстенсивный и интенсивный пути развития ставят совершенно разные проблемы при обеспечении безопасности информационного взаимодействия.

Разработка действительно интеллектуальных систем сегодня является нерешенной задачей. Все инновации последних десятилетий развития человечества, направленные на создание информационных продуктов и услуг, поддержку информационного взаимодействия между людьми и обеспечение свободного доступа к мировым информационным ресурсам, основаны на совершенствовании физической среды взаимодействия и автоматизации информационных процессов материального метауровня. Поэтому новые вызовы для специалистов в области безопасности возникали каждый раз при переходе на новый этап развития технологий инфокоммуникации.

Технология инфокоммуникации появилась на рубеже веков как результат конвергенции услуг систем сохранения данных, телекоммуникаций и вычислительной техники. Сегодня инфокоммуникация стала доминирующей областью деятельности человека и может быть названа технологией XXI века [1],[8]. Не случайно годовой доход инфокоммуникационного сектора экономики, в который включают телекоммуникационные услуги, производство электронного оборудования, вычислительной техники и программного обеспечения [9], измеряется в сотнях миллиардов долларов и темпы их развития опережают другие отрасли. Инфокоммуникации существенно меняют не только способ производства продуктов и услуг, но и служат основой общественного развития.

Широкое внедрение средств информатизации определило переход от индустриального к информационному обществу. Можно предположить, что следующим этапом развития человечества будет связан с появлений интеллектуальных технологий, которые станут основой новых производственных отношений и приведут к формированию интеллектуального общества [10].

Такое движение в текущем тысячелетии предвидел В.И. Вернадский, который назвал новую среду обитания человека ноосферой [11]. С информационно-технологической точки зрения ноосфера должна пройти два этапа развития – материальный и интеллектуальный. Первый обеспечивает накопление глобального информационного ресурса благодаря целенаправленной деятельности многих поколений людей [2].

Становление информационного общества можно рассматривать как многоэтапный процесс накопления информационного ресурса, включающий этап языкового взаимодействия людей и цивилизаций, этап массового создания и тиражирования информации и, наконец, этап массового доступа к информационным ресурсам при помощи инфокоммуникационных технологий.

В настоящее время уже накоплены настолько большие объемы информационного ресурса, что проблемой становится не только обеспечение безопасности этих ресурсов, но и сложность доступа к данным в процессе удовлетворения информационных потребностей людей [12].

Второй уровень ноосферы нужно понимать как интеллектуальный. Он может быть достигнут на базе накопленных информационных ресурсов при условии, что этот ресурс эффективно сохраняется во времени, распространяется в пространстве и обрабатывается при решении многообразных задач с применением качественно новых интеллектуальных технологий и систем во благо развития цивилизации. Переход от информационного к интеллектуальному обществу станет одним из

результатов такого развития и приведет к новым угрозам и качественному усложнению задач обеспечения информационной безопасности.

Данные исследований и прогнозные оценки о растущих объемах информации в XXI веке (например [13]) подтверждают предположения В.И. Вернадского. Так, например, за один 1999 год, последний год XX века, в мире было произведено от 2 до 3 Экзабайт данных. В 2002 году уже от 3 до 5 Экзабайт, а в 2011 году объем цифровой информации в 10 раз превысил объем 2006 года. По прогнозам, к 2020 г. объем информации достигнет 40 Зеттабайт [14].

Сегодня темпы производства новой информации в 30 раз выше, чем в XIX-м веке. Объем информации удваивается в последние годы каждые 20 месяцев против 50 лет (или шестисот месяцев) в XIX-м веке [14]. Во 2-м десятилетии XXI века динамика роста информации стала еще выше.

Такие процессы наблюдаются практически во всех сферах деятельности человека: культуре, экономике, политике, науке, образовании и других. Возрастающий объем информационного ресурса вовлекает в информационную индустрию все большее количество людей. Доля людей, занятых в сфере производства и распространения информации, значительно выше, чем в других видах человеческой деятельности. Более того, свыше 60% новых рабочих мест в развитых странах связаны сегодня с той или иной формой преобразования информации.

Переход к информационному обществу на базе технологий инфокоммуникации привел к коренной перестройке всех основных социально-экономических структур, к росту интеллектуальной составляющей трудовой деятельности, к изменению общественной роли членов общества. Изменились цели, приоритеты, проблемы и стандарты общественной жизни.

Экономика информационного общества ориентирована на стремительный рост информационных ресурсов, на постоянное изменение внешней обстановки и отличается мобильностью. Основные экономические признаки информационного общества являются следствием широкого внедрения и доступности конвергентных инфокоммуникационных систем [14].

Для создания эффективной системы использования и защиты информационных ресурсов, рынка, производства, инфраструктуры и технологий в России принята государственная программа «Информационное общество (2011-2020)». Главная идея реализуемого в ее рамках нового подхода заключается в том, что ценность представляют не внедренные технологии и разработанные информационные системы сами по себе, а то, какую пользу они приносят гражданам, бизнесу, всему обществу [15].

Цель программы – получение гражданами и организациями преимуществ от применения информационных и телекоммуникационных технологий – предполагает решение трех взаимосвязанных задач:

– обеспечение предоставления гражданам и организациям услуг с использованием современных информационных и телекоммуникационных технологий;
– развитие технической и технологической основы становления информационного общества;
– предупреждение угроз, возникающих в информационном обществе.

Необходимым условием решения двух последних задач является создание сверхмощных инфокоммуникационных систем – центров обработки данных и суперкомпьютеров [16, 17]. Эти технологии относятся к числу стратегических. Без них невозможно, с одной стороны, развитие авиастроения, атомной энергетики, автомобилестроения, ракетно-космической техники и других наукоемких отраслей экономики, имеющих первостепенное значение для безопасности государства, а, с другой стороны, контроль за безопасностью информационного взаимодействия. Например, проект приказа Минкомсвязи (апрель 2013 г.) обязывает операторов связи передать спецслужбам, ответственным за информационную безопасность, контролируемый ими трафик интернет. Он должен храниться в специальных центрах и быть доступным для анализа не менее 12 часов. Это значит, что каждые 12 часов сети связи, системы хранения и обработки должны «осваивать» в реальном времени примерно 30-40 Пбайт данных, что соответствует потоку данных интенсивностью примерно 1 Тбит/с. Такая производительность по силам лишь самым совершенным супервычислителям.

Увеличение производительности суперкомпьютеров требует увеличения числа вычислительных узлов, их надежности и развития методов программирования параллельных вычислений, однако главным резервом увеличения производительности является развитие инфокоммуникационных свойств, которые приводят к уменьшению времени доступа при обращении к памяти и к коммутационной сети для перемещения данных между вычислительными узлами.

Фундаментальное значение для успешного выполнения государственной программы имеет совершенствование технологий построения физической среды взаимодействия (рис. 1), инструментальным компонентом которой являются цифровые средства информатизации. В основе этих средств лежат достижения в области электроники, фотоники и радиотехники.

Электроника обеспечивает аппаратную платформу для решения задач сохранения и обработки информации. В 1964 году важный технологический принцип, в последствие подтвержденный практикой, сформулировал Г. Мур: «Производительность кремниевых интегральных микросхем и количество транзисторов на одном кремниевом кристалле будут удваиваться каждые 18 месяцев, а их стоимость при этом будет уменьшаться в два раза». Это означает, что возможности аппаратной

платформы для создания компьютерных технологий растут примерно такими же темпами, как и объем информационного ресурса в обществе. Уже сегодня стала возможна реализация сложнейших электронных изделий на одном чипе при значительном расширении их функциональных возможностей, например: емкость оперативной памяти компьютера достигает нескольких террабит, что соизмеримо с возможностями мозга человека при сохранении информации; производительность персонального компьютера измеряется в 109 флопс, а суперкомпьютеров достигает 1015 флопс и выше; кристалл современного процессора содержит ~1,5 млрд. транзисторов, что позволяет создавать сложные многоядерные архитектуры; существенно уменьшается мощность, потребляемая электронными устройствами.

Главный резерв улучшения характеристик электронных компонент связан с наноэлектроникой – областью электроники, где создают интегральные электронные схемы с топологическими размерами элементов менее 0,1 мкм. Современный техпроцесс уже достиг показателя 22 нм. В перспективе технология может перекрыть весь диапазон размеров вплоть до атомарного.

Одновременно увеличивается объем информации, который может быть сохранен на долговременных цифровых информационных носителях. Максимальная теоретическая плотность данных в случае использования магнитной записи с подогревом (технология HAMR) в ближайшее время составит 5-20 Тбит на квадратный дюйм. Предполагается, что в 2014 году емкость твердотельного накопителя SSD приблизится к 16 Тбайт. Согласно новому открытию, можно синтезировать частицу ДНК и записать в нее Экзабайты данных и сохранять их теоретически тысячи лет в лиофилизированной форме.

На смену кремниевым технологиям должны придти оптические и квантовые методы обработки и сохранения данных.

Фотоника объединяет разнообразные технологии создания волоконно-оптических линий связи (ВОЛС) от изготовления лазера до производства оптического волокна. Для ВОЛС также характерно увеличение объемных характеристик при уменьшении относительной стоимости систем. Пропускная способность коммерческих ВОЛС удваивается за 1 год, т.е. растет даже быстрее, чем производительность электронных устройств и в два раза быстрее, чем объем информационного ресурса в обществе. Эти темпы должны сохранится в течении следующих примерно 10 лет.

Уже сегодня технологии модуляции позволяют получить скорость передачи в несколько Тбит/с в одном волокне без переприема при передаче информации на расстояние до 100 км. Это означает, что всю информацию, которую способен запомнить человек или весь мировой объем междугородного и международного трафика можно передать на значительные расстояния по одному волокну за несколько секунд.

Технологии построения ВОЛС приводят к снижению стоимости передачи 1 бита информации. В результате затраты на распространение данных перестали зависеть от расстояния между взаимодействующими терминалами.

Главный резерв увеличения эффективности оптических систем заключается в отказе от опто-электрических и электро-оптических преобразований на этапах усиления и ввода/вывода сигналов. С этой целью разрабатываются новые типы лазеров, оптические регенераторы, маршрутизаторы, процессоры и другие оптические устройства. В перспективе возможна полная замена электронных технологий на оптические.

Достижения в области радиотехники привели, в частности, к появлению мобильных сетей (сетей связи с подвижными объектами). В последние годы изменилась роль и место, которое они занимают в общей архитектуре инфокоммуникационных технологий. Количество мобильных подключений в мире сравнялось с количеством фиксированных еще в 2004 году, а в 2012 году превысило 5 млрд. Мобильные сети стали универсальным средством доступа пользователей к глобальным сетям, информационным услугам и контенту. Возможности мобильной передачи экономической информации, в первую очередь мобильные платежи, когда мобильный телефон заменит и наличные деньги и кредитные карты, существенно повлияют на технологии ведения бизнеса [1].

Для того чтобы мобильные сети заменили привычный стационарный доступ для получения услуг TriplePlay необходимо увеличение спектральной эффективности. Ключевыми факторами здесь являются методы сжатия сигналов, их кодирования и обработки и построения нового типа множественных приемо-передающих антенн. Использование этих методов позволит приблизить спектральную эффективность к ее теоретически возможным значениям.

Заключение. Из проведенного анализа следует, что технологическая основа информационного общества была создана благодаря поэтапному развитию цифровых технологий сохранения, распространения и обработки информации и их конвергенции в инфокоммуникационных системах, в частности, в центрах обработки данных и суперкомпьютерах.

До сих пор эти технологии развивались по экстенсивному пути, совершенствовались в основном с точки зрения объемных характеристик, таких как объем записей в системах хранения, пропускная способность систем распространения, производительность систем обработки данных.

Сегодня технологические проблемы сохранения, распространения и обработки больших объемов информационного ресурса можно считать решенными, что, соответственно, позволяет четко

очертить круг проблем, которые стоят перед специалистами в области информационной безопасности на материальном метауровне информационного взаимодействия. Основная сложность здесь – это масштаб информационного пространства, который требует создания соответствующих по масштабу систем безопасности.

Для перехода к интеллектуальному обществу необходимо интенсивное развитие. Это означает, что должна появиться новая интеллектуальная, возможно не цифровая, технология работы с информацией. Внедрение интеллектуальных информационных систем сделает проблему информационной безопасности не разрешимой при помощи используемых сегодня методов и средств. Проблема информационной безопасности на идеальном метауровне при условии появления машин, имеющих интеллектуальный потенциал, соизмеримый с человеческим, пока наукой даже не сформулирована.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю.Ф., Колбанёв М.О. Технология инфокоммуникации. – Курск: Науком, 2011. – 260 с.
2. Советов Б. Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность, №1, 2014. С. 69-77.
3. Татарникова Т.М. Защищенные корпоративные сети: задачи по защите информации. – СПб: РГГМУ, 2012. – 113 с.
4. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Двухуровневая модель информационного взаимодействия// VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013. С 184
5. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – 830 с.
6. Советов Б.Я., Цехановский В.В., Чертовской В.Д. Интеллектуальные системы и технологии. – М.: Академия, 2013. – 320 с.
7. Колбанёв М.О., Яковлев С.А. Модели и методы оценки характеристик обработки информации в интеллектуальных сетях связи. – СПб.: СПбГУ, 2002. – 230 с.
8. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. О развитии технологии информационного общества// VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013. С 23
9. Кондратьев В.Б. Сектор информационных технологий правит миром. – Портал «Перспективы», http://www.perspektivy.info. 2011.
10. Советов Б.Я. Проблемы перехода к ноосферному образованию//4-я международная научно-практическая конференция «Ноосферное образование в Евразийском пространстве». – СПб., 2012 – 0,5 п.л.
11. Вернадский В.И. Биосфера и ноосфера / Предисловие Р.К. Баландина. – М.:Айрис-пресс, 2004.- 576 с.
12. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Оценка вероятности эрланговского старения информации//Информационно-управляющие системы, №6, 2013. С. 25-28.
13. Martin H., Priscila L. The World's Technological Capacity to Store, Communicate, and Compute Information//Science 1 April 2011: Vol. 332 no. 6025 pp. 60-65.
14. Абдеев Р.Ф. Философия информационной цивилизации. - М.: ВЛАДОС, 1994.
15. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. N 1815-р г. Москва «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)».
16. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель балансировки нагрузки в вычислительном кластере центра обработки данных//Информационно-управляющие системы. 2012 № 3(58). С. 37-41.
17. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель обработки клиентских запросов//Телекоммуникации. 2013 №9. С. 42-48.

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ

УДК 004.94

ИНТЕГРАЦИЯ ПОДСИСТЕМ И СЕРВИСОВ ДОСТУПА К РЕЗУЛЬТАТАМ КОСМИЧЕСКОГО МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ[1]

Зеленцов Вячеслав Алексеевич[1], Ковалев Александр Павлович[2], Кожанов Александр Николаевич[1], Пиманов Илья Юрьевич[1], Потрясаев Семен Алексеевич[1], Скобцов Вадим Юрьевич[3],
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия В.О., д. 39,
Федеральное государственное унитарное предприятие
«Конструкторское бюро «Арсенал» имени М.В. Фрунзе»
Россия, Санкт-Петербург, ул. Комсомола, 1-3,
[3]Объединенный институт проблем информатики Национальной академии наук Беларуси,
Беларусь, 220012, Минск, ул. Сурганова, 6,
e-mails: v.a.zelentsov@gmail.com, e.plahotnik@mail.ru, kan_spb@mail.ru, pimen@list.ru,
spotryasaev@gmail.com, vasko_vasko@mail.ru.

Аннотация: В статье рассмотрены базовые подходы к решению проблемы интеграции сервисов, предоставляемых различными системами мониторинга и внешними информационными системами при решении задач прогнозирования чрезвычайных ситуаций. Показана необходимость и возможность реализации принципа «одного окна» при обращении к разнородным информационным ресурсам и моделям расчета параметров стихийных бедствий.

Ключевые слова: *интеграция, геосервисы, мониторинг, прогнозирование, чрезвычайные ситуации.*

INTEGRATION OF SUBSYSTEMS AND SERVICES FOR ACCESS TO THE RESULTS OF EMERGENCIES SPACE MONITORING AND FORECASTING[1]

Viacheslav Zelentsov[1], Aleksandr Kovalev[2], Aleksandr Kojanov[1], Ilja Pimanov[1],
Semen Potryasaev[1], Vadim Skobtsov[3]
[1] St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
[2]Design Bureau "Arsenal",
[3] The United Institute of Informatics Problems of the National Academy of Sciences of Belarus,
e-mails: v.a.zelentsov@gmail.com, e.plahotnik@mail.ru, kan_spb@mail.ru, pimen@list.ru,
spotryasaev@gmail.com, vasko_vasko@mail.ru.

Abstract: The basic approaches to the integration of services provided by different monitoring systems and external information systems to solve the problems of emergency situations forecasting are considered. The necessity and the possibility of implementing the "single window" principle when users refer to heterogeneous information resources and models for calculating the parameters of natural-technological disasters are shown.

Keywords: *integration, geoservices, monitoring, forecasting, emergencies.*

Введение. В настоящее время активно развивается большое число проектов и систем космического мониторинга чрезвычайных ситуаций (ЧС) различного характера – как природных, так и техногенных. На международном уровне наиболее значимыми являются проекты GEOSS, GMES (COPERNICUS), Хартия «SPACE & MAJOR DISASTERS», проект «SANTINEL ASIA». С запуском в 2012 году первого российского спутника серии «Канопус» создание космической системы мониторинга чрезвычайных ситуаций началось в рамках Союзного государства России и Белоруссии.

В РФ для решения задач не только мониторинга, но и прогнозирования возникновения и

[1] Работа выполнена при финансовой поддержке Программы НТС Союзного государства «Мониторинг СГ» (проект 1.4.1–1), грантов РФФИ №№12-07-00302, 13-07-00279, 13-08-00702, 13-08-01250, 13-07-12120, 13-06-0087, 15-07-01230, Программы фундаментальных исследований ОНИТ РАН (проект №2.11), СЧ НИР «Планета-ПМ-СП».

развития ЧС реализуется проект создания Международной аэрокосмической системы глобального мониторинга (МАКСМ) [1] и ее фрагментов для различных отраслей и видов ЧС, в частности, наводнений, лесных пожаров, землетрясений, контроля и сопровождения критически важных объектов и особо опасных грузов.

Дальнейшее развитие существующих систем и создание новых приводит, с одной стороны, к большей детализации информации о ЧС и увеличению ее количества, что должно способствовать улучшению качества принимаемых решений по снижению негативных последствий от ЧС, а с другой стороны, эти обстоятельства ведут к усложнению процедур получения необходимой информации пользователям, поскольку для оценки ситуации на одной и той же территории приходится обращаться одновременно к большому количеству систем и предоставляемых ими сервисов.

При этом необходимо отметить, что повышение достоверности решения задач прогнозирования ЧС требует комплексного применения не только космических, но и наземных, а также авиационных средств измерений и обработки данных. Состав привлекаемых данных и источники их получения, естественно, зависит от типа рассматриваемой ЧС.

В частности, в РФ деятельность по мониторингу и прогнозированию чрезвычайных ситуаций осуществляется целым рядом организаций. Так, например, мониторинг и прогноз событий гидрометеорологического характера проводят структуры Росгидромета. Сейсмические наблюдения и прогноз землетрясений осуществляются Федеральной системой сейсмологических наблюдений, в которую, входят учреждения и наблюдательные сети РАН, МЧС, Минобороны, и др. Определённую роль в осуществлении мониторинга и прогнозирования ЧС играет Минприроды, которое осуществляет общее руководство государственной системой экологического мониторинга, а также координацию деятельности в области наблюдений за состоянием окружающей среды. Применительно к рассматриваемой проблематике его учреждения организуют мониторинг: источников антропогенного воздействия на природную среду, а также прогнозирование опасных экзогенных/эндогенных геологических процессов. Мониторинг состояния техногенных объектов и прогноз аварийности организует и осуществляет Федеральная служба по экологическому, технологическому и атомному надзору.

В этих условиях одной из ключевых проблем создания перспективных систем космического мониторинга и прогнозирования ЧС становится необходимость интеграции данных и информации, получаемых из различных источников, а также интеграции подсистем доступа и доведения результатов мониторинга и прогнозирования ЧС до потенциальных потребителей.

Существующие подходы к реализации подсистем и сервисов предоставления результатов мониторинга. В настоящее время в Российской Федерации создано большое количество интернет-сервисов и геопорталов, предоставляющих разнообразную информацию с результатами мониторинга различных природно-технологических объектов и процессов. Среди них можно выделить несколько решений всероссийского и международного уровня, такие как геопортал Роскосмоса (http://gptl.ru/), информационную систему дистанционного мониторинга Федерального агентства лесного хозяйства (http://www.nffc.aviales.ru/), информационный ресурс системы космического мониторинга чрезвычайных ситуаций «Каскад» (http://www.ukmmchs.ru/), геопортал «Вега» Института космических исследований РАН (http://pro-vega.ru/), тематические порталы на базе ресурса «Космоснимки» НТЦ СканЭкс (http://kosmosnimki.ru/), и другие.

Несмотря на большой объём и разнообразие собираемых, обрабатываемых и распространяемых данных, на современном этапе развития отечественных систем мониторинга существует ряд проблем, препятствующих интегрированному использованию этих данных при решении задач мониторинга и прогнозирования ЧС.

Во-первых, подавляющее большинство существующих систем ориентировано исключительно на человеко-машинный интерфейс и в конечном итоге формирует на веб-странице изображение, содержащее представление требуемых пространственных данных. Очевидно, в этом случае их дальнейшее использование для автоматизированного решения прикладных задач становится невозможным.

Во-вторых, известны лишь единичные случаи предоставления моделей предметных областей как сервиса для работы с пользовательскими данными. То есть, большинство порталов предоставляют доступ к результатам расчётов, и у пользователя сервиса нет возможности выполнить новый расчёт с другими исходными данными.

В-третьих, зачастую первичные исходные данные, на основе которых формировались предоставляемые порталом данные с результатами мониторинга, имеют большое значение для конечного пользователя. Сюда можно отнести показания всевозможных датчиков, результаты измерений различных параметров сложных природно-технологических объектов. В большинстве существующих систем мониторинга эти данные сами по себе не предоставляются.

Другим важным вопросом является контроль доступа к наборам данных с промежуточными и конечными результатами обработки и мониторинга. Каждая упомянутая выше система использует собственный механизм разграничения доступа и способ аутентификации. В связи с этим отсутствует возможность использовать технологию единого входа (Single Sign-On), когда пользователь переходит

из одного раздела портала в другой без повторной аутентификации. Этот вопрос имеет особую важность в случае, если пользователю необходимо автоматически регулярно получать данные из нескольких сервисов мониторинга.

Таким образом, несмотря на появление единичных случаев разработки современных высокотехнологичных геосервисов с соблюдением стандартов веб-картографии и использованием подходов разделения данных и их представления, большинство существующих порталов-поставщиков данных мониторинга на данный момент не ориентированы на работу в качестве составных частей (функциональных модулей) в информационных системах конечных потребителей.

Федеральной космической программой предусмотрено создание Единой территориально-распределенной информационной системы дистанционного зондирования Земли (ЕТРИС ДЗЗ) [2] для обеспечения радикального решения этой проблемы, что среди прочего подразумевает диверсификацию форм взаимодействия будущих операторов и пользователей космической информации.

Но для решения всего комплекса проблем предоставления пользователям необходимых продуктов и сервисов необходимо при создании при создании перспективных космических систем мониторинга и прогнозирования обеспечить интеграцию ресурсов и сервисов ЕТРИС ДЗЗ, отраслевых и территориальных систем мониторинга, а также вновь создаваемых информационных ресурсов, причем «бесшовно» для конечного пользователя. Целевой пользователь не должен решать задачи выбора какой-либо конкретной системы мониторинга для получения результата прогнозирования, его интерфейс должен быть максимально прост и настроен на возможность описания постановки задач и запроса на языке предметной области (сейсмопрогноз, прогноз наводнений, и т.д.).

Предлагаемые подходы к интеграции подсистем и сервисов доступа к результатам мониторинга и прогнозирования. Базовый принцип, который положен в основу решения задач интеграции подсистем и сервисов доступа в современных информационных системах, в том числе в перспективных системах мониторинга и прогнозирования – это максимальная автоматизация. Под автоматизацией понимается соответствующий уровень организации как человеко-машинных, так и машинно-машинных интерфейсов между поставщиками и потребителями результатов мониторинга. Автоматизация становится возможной при использовании всеми участниками информационного обмена стандартных протоколов доступа к информации. Унификация доступа к данным позволяет получать их из авторизованного первоисточника. Становится возможной каталогизация данных мониторинга без переноса их в централизованную систему, что значительно повышает актуальность этих данных. Конечный пользователь, в свою очередь, получает интерфейс для поиска требуемого сервиса среди большого количества различных поставщиков. Всё это приводит к практической реализуемости принципа «одного окна» для простого доступа к колоссальному объёму актуальной информации с результатами измерений, обработки данных, и расчетов. Описанный подход при интегрированном использовании данных дистанционного зондирования Земли (ДЗЗ) и гидрологических моделей для целей прогнозирования наводнений проиллюстрирован на рисунке 1.

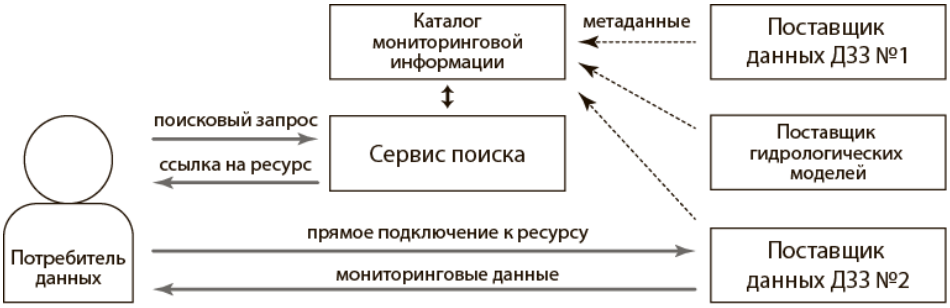


Рис. 1. Принцип «одного окна» для доступа к результатам мониторинга и прогнозирования

При решении различных задач мониторинга и прогнозирования ЧС возникает потребность не только в данных ДЗЗ, но и в ряде сведений о территории, например, адресные планы, объекты инфраструктуры, электролинии, трубо- и газопроводы, другие коммуникации, состав леса, половозрастной состав населения, и многое другое. Подобные сведения хранятся в информационных системах администраций муниципальных образований, государственных комитетов, эксплуатирующих организаций. Использование указанных сведений позволяет решать задачи, связанные с ЧС, их мониторингом и прогнозированием, на более высоком качественном уровне, принимать решения более оперативно и обосновано.

Первым шагом на пути к интеграции подсистем и сервисов доведения разнородных данных является обязательное использование стандартов веб-картографии [4] всеми задействованными поставщиками этих данных.

К настоящему времени наибольшее признание получили стандарты, разработанные непрофильной международной, добровольной организацией Open Geospatial Consortium (OGC) , являющейся объединением более 450 компаний, правительственных учреждений и университетов.

Подавляющее большинство функционирующих сейчас систем доведения пространственных данных до потребителя используют следующие спецификации OGC:

– Web Map Service (WMS) – предоставляет собой простой интерфейс запроса к цифровой карте, содержащей изображения из одной или нескольких распределенных геопространственных баз данных. В ответе на запрос возвращаются данные в растровом виде (все изображения, соответствующие параметрам запроса), которые могут быть отображены в пользовательском приложении. Интерфейс также поддерживает возможность указать, будут ли возвращенные изображения объединены, если они принадлежат разным серверам;

– Web Feature Service (WFS) – описывает стандартный интерфейс доступа и манипуляции с географическими объектами с помощью запросов. Стандарт предполагает, что на выходе WFS-сервис отдает векторные данные (геометрию и атрибуты).

Кроме того, необходимо использовать дополнительные возможности, предоставляемые многими геоинформационными серверными решениями:

– Web Coverage Service (WCS) – расширяет возможности WMS для предоставления растровой географической информации, поддерживает функции электронного поиска цифровой геопространственной информации, представляющей пространственно-временное изменение явлений, WCS разрабатывается для представления свойств и значений в каждой конкретной точке географического пространства, а не на создание готовых картинок, а также позволяет проводить интерпретацию данных не на сервере, а на клиентской части приложения.

Указанные стандарты нацелены на предоставление и простейшую модификацию пространственных данных. Помимо этого, поставщики данных мониторинга могут предоставлять более сложные геосервисы по обработке исходных данных. Их интеграция становится возможной благодаря наличию стандарта WPS (веб-сервис геопроцессинга), который описывает правила для входящих и исходящих данных (запросов и ответов на них) для сервисов геопроцессинга (геообработки). Геопроцессинг может включать любой алгоритм, расчёт или модель, оперирующие векторными или растровыми данными с пространственной привязкой. WPS может описывать как простые расчёты, такие, как вычитание одного набора пространственных данных из другого, так и более сложные, такие, как модели сейсмопрогнозирования, мониторинга и прогнозирования лесопожарной и гидрологической обстановки. Таким образом, конечному потребителю предоставляются не просто данные, а сервис по выполнению расчётов с использованием сложных алгоритмов и вычислительных мощностей центров обработки данных. Этот вид сервиса важен, например, при выполнении потребителем сценарного моделирования «что - если» различных вариантов возведения противопаводковых защитных сооружений. Птребитель сервиса может использовать гидрологические модели, расположенные в центрах обработки данных, для выполнения собственных расчётов.

Для организации доступа к остальным сервисам, результатом работы которых не является геопространственная информация, следует использовать сервис-ориентированную архитектуру построения информационной системы [5], [6]. Такой подход позволит преобразовать массу частных программных интерфейсов поставщиков данных и сервисов к единому стандартному виду. Так, сервисная шина в рамках сервис-ориентированной архитектуры даёт возможность с «внутренней» стороны использовать протоколы REST API, подключения к серверам FTP и HTTP, обработку файлов XML, отправку запросов во всевозможные СУБД поставщиков данных, а с «внешней» стороны предоставлять документированный веб-сервис, принимающий запросы и возвращающий результат по стандартному протоколу SOAP.

Кроме простого преобразования запросов, благодаря использованию сервис-ориентированной архитектуры становится возможным визуальное конструирование алгоритмов работы с данными с задействованием различных источников и сервисов. Применение языка исполнения бизнес-процессов (Business Process Execution Language, BPEL) позволяет организовать логику выполнения ряда веб-сервисов, используя, в том числе, визуальный редактор [7], [8]. Таким образом, конечному потребителю могут быть предоставлены данные и информация различного уровня обработки, сформированные «на лету».

При переходе от массы частных интерфейсов к единому появляется возможность включать веб-сервисы в каталог и осуществлять по ним поиск. Пример работы описанной схемы приведён на рисунке 2.

Важным фактом является то, что отдельные поставщики данных и их геопорталы продолжают существовать в привычном для пользователя виде. Использование стандартов веб-картографии и веб-сервисов не подразумевает отказ от собственных пользовательских интерфейсов, а лишь предоставляет дополнительные возможности. Так, одни поставщики данных мониторинга, имея договорённости с другими поставщиками, получают удобный способ отображения пространственных данных друг друга на своих геопорталах. При этом отсутствует необходимость переносить какие-либо

архивы с данными, так как вся необходимая информация будет предоставляться в режиме «он-лайн». С точки зрения конечного пользователя работа геопортала не зависит от физического расположения предоставляемых данных.

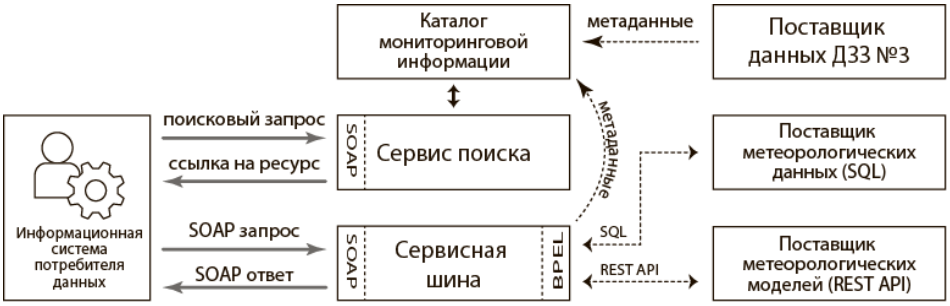


Рис. 2. Пример предоставления синтезированного сервиса.

С учётом описанных выше подходов и принципов можно требования к сервисам и продуктам отдельных поставщиков данных, используемых в интегрированной системе доведения до потребителей результатов мониторинга и прогнозирования:

1. Наличие у предоставляемого сервиса программного интерфейса, то есть, возможности взаимодействия с сервисом без участия пользователя. В противном случае становится невозможным использование сервиса в информационных системах пользователя, выполняющих регулярное автоматическое решение прикладных задач.
2. Разделение данных и их представления. Данные, встроенные в гипертекстовую разметку на стороне сервера, требуют высокой трудоёмкости для их автоматического извлечения, поэтому требуется строго отделять данные от их внешнего представления пользователю.
3. Использование для передачи текстовых данных стандартных форматов, таких как XML или JSON. Большинство информационных систем потребителей уже имеют встроенную поддержку этих форматов. Применение собственных форматов данных может значительно усложнить взаимодействие систем.
4. Наличие механизмов автоматической аутентификации. Предпочтительно использование механизмов, поддерживающих единый вход (Single Sign-On): стандарт SAML (Security Assertion Markup Language), стандарты WS-Trust и WS-Federation для SOAP/XML-веб сервисов, стандарты OAuth и OpenID Connect.

Соблюдение поставщиками этих базовых требований позволит провести интеграцию различных подсистем доведения информации до потребителей и предоставить конечному потребителю удобный и функциональный сервис доступа к результатам мониторинга и прогнозирования.

Заключение. Предложенные подходы к интеграции подсистем и сервисов к результатам мониторинга и прогнозирования ЧС позволяют устранить противоречие между существующим колоссальным объёмом мониторинговых данных различной природы и уровней обработки, и организацией доступа к этим данным, что должно существенно повысить качество принимаемых решений по предупреждению и снижению негативных последствий от ЧС. Перспективная интегрированная подсистема распространения результатов мониторинга и прогнозирования, основанная на предлагаемых подходах, обеспечивает реализацию принципа «одного окна» и предоставление потребителям удобные сервисы поиска требуемого источника данных в актуальном каталоге, доступ к данным на основе стандартов веб-картографии и веб-сервисов, а также обеспечивает разграничение прав доступа к данным и сквозную аутентификацию пользователя.

При этом предлагаемые подходы к интеграции подсистем и сервисов доступа носят достаточно общий характер и применимы для решения задач создания интегрированных геосервисов для широкого класса территориально распределенных информационных систем различного назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Меньшиков В.А., Пушкарский С.В., Зеленцов В.А. Проект создания Международной аэрокосмической системы глобального мониторинга: современное состояние и перспективы реализации // Геополитика и безопасность, 2011, №4(16). – С. 92-101.
2. Лошкарев П.А., Тихоян О.О., Курлыков А.М., Кошкин А.В., Гладков А.П. Развитие ЕТРИС ДЗЗ с применением облачных технологий. // Геоматика, 2013, №4, с.22–26.
3. Зеленцов В.А., Ковалев А.П., Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Методология создания и применения интеллектуальных информационных технологий наземно-космического мониторинга сложных объектов // Труды СПИИРАН, 2013, выпуск 5(28), с. 7–81.
4. Рогачев С.А. Веб-картография. Представление разнородной пространственной информации // Труды СПИИРАН, 2013, выпуск 6(29), с.132–143.
5. Компас в мире сервис-ориентированной архитектуры (SOA): ценность для бизнеса, планирования и план развития предприятия / Н.Биьерштейн, С.Боуз, К.Джонс и др.: пер. с англ. – М.: КУДИЦ-ПРЕСС, 2007.
6. Дмитров А. Сервисно-ориентированная архитектура в современных моделях бизнеса. – М.: 2006, 224с.
7. Vasiliev, Y.: SOA and WS-BPEL: Composing Service-Oriented Solution with PHP and ActiveBPEL. Packt Publishing, 2007.
8. Юдицкий С.А. Сценарный подход к моделированию поведения бизнес-систем. – М.: СИНТЕГ, 2001. – 112 с.

УДК 681.3

МЕТОДИКА ГАРАНТИРОВАННОГО ВЫПОЛНЕНИЯ ЗАДАЧ ПРИ РАССТАНОВКЕ ПО ПРОЦЕССОРАМ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ

Калачева Светлана Борисовна,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия В.О., д. 39,
e-mail: svet@iias.spb.su

Аннотация: Системы реального времени (СРВ) широко используются в современной технике. Основная проблема при их использовании – выполнимость набора компьютерных задач в указанные сроки. В статье исследуется жесткая СРВ, в которой время отклика задачи не превышает периода выполнения задачи. Рассмотрена методика выбора метода расстановки требуемого набора задач СРВ по процессорам в многопроцессорных системах для обеспечения его выполнимости. Приведен иллюстрирующий пример.

Ключевые слова*: системы реального времени, многопроцессорные системы, планирование заданий, выполнимость заданий.*

METHOD OF THE GARANTEE TASK FULFILING WHEN DISTRIBUTION ON THE PROCESSORS IN THE REAL-TIME APPLICATION

Svetlana Kalacheva,
St.Petersburg Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line, 39,
e-mail: svet@iias.spb.su

Abstract: The real-time application wide utilize in the modern utilizing. The main problem when they are used is the task collection feasibility of the computer task set in the fixed period. In the article the strict real-time application is described, i. e. the time of the task response should not be more then the period of the task. In the paper the principles of the selection of the planning method for the allocation of the task collection in the real-time application in the multiprocessing systems for the tasks feasibility providing is described. The adducing of instance takes place.

Keywords*: real-time systems, multiprocessors systems, task scheduling, task feasibility.*

Введение. Компьютеры с операционной системой реального времени широко используются в современных технических приборах, так как обеспечивают гарантированное выполнение повторяющихся наборов компьютерных задач. Различают несколько дисциплин планирования выполнения таких наборов задач. Наиболее распространенным методом является метод RM-планирования [2]. Кроме него, используется метод DM-планирования [1], в котором введено более жесткое ограничение на время отклика задачи. С появлением многопроцессорных систем были разработаны методы расстановки задач по процессорам с помощью программы-планировщика периода выполнения задач. Было выявлено что набор задач при довольно низкой суммарной загрузке процессоров является невыполнимым (эффект Дала [3]). Для предотвращения этого следует присваивать наиболее высокий приоритет задачам с большим периодом [7]. Кроме того, были разработаны другие методы планирования, позволяющие реализовать наиболее полное использование мощности процессора при обеспечении своевременного выполнения всех заданий [6], в том числе и Pfair-планирование [1]. Однако этот метод не сохраняет приоритеты задач во время моделирования. От этого недостатка свободен другой разработанный метод сохраняющий приоритеты задач во время всего процесса моделирования – это метод RM_US-планирования [4].

Данное исследование является продолжением и развитием исследования методов планирования, приводящих к выполнению наборов задач в СРВ на нескольких процессорах [8].

Основные понятия и используемые методы. Постановка задачи. Задачи из выполняемого набора задач $\{\tau_1, \tau_2, ...\tau_n\}$ принято обозначать τ_i [1]. Они характеризуются двумя величинами: периодом выполнения i-й задачи, который обозначается, T_i и временем выполнения i-й задачи, которое обозначается как C_i Отношение времени выполнения задачи к ее периоду называют нагрузкой и обозначают u_i [1]. В момент времени, равный нулю, а также в каждый момент времени, кратный T_i по задаче τ_i генерируется задание τ_i^j задачи τ_i. Время с начала порождения задания до его завершения называется временем отклика задания и обозначается r_i^j [1].

Набор задач называется выполнимым на наборе процессоров, если для каждого задания выполняется условие, что максимальное значение времени отклика задания не превосходит периода выполнения задачи [1]. Рассматривается жесткая СРВ – то есть максимальное значение времени отклика заданий данной задачи не должны превосходить ее периода:

$$\max_j r_i^j \le T_i .$$

Кроме того, рассматриваются дисциплины планирования с неизменными приоритетами задач.

Полученные значения ранжируются; определяется максимальное и минимальное значение периода и времени выполнения задачи, затем они округляются до сотен микросекунд для определения более короткого интервала моделирования, когда повторяется вновь выстраивание всех заданий на старте (в общем случае требуемый интервал моделирования получался перемножением значений периодов всех задач, а так учитывались общие знаменатели). Таким образом, рассматриваются всевозможные сочетания заданий, и максимальное время отклика получалось для округленных значений точно.

Наиболее часто используемыми методами планирования выполнения наборов задач, сохраняющими приоритет задач, являются методы RM-планирования [2] и RM_US-планирования [4].

Метод RM-планирования – это метод частотно-монотонного планирования, используемый и в однопроцессорных системах. Приоритет задачи тем выше, чем меньше ее период. Расстановка задач по процессорам в многопроцессорной системе выполняется планировщиком периода разработки набора задач. При использовании метода RM_US-планирования множество $\{\tau_1, \tau_2, ...\tau_n\}$ задач разбивается на следующие два подмножества [5]:

1. Старшие задачи $\{\tau_1, \tau_2, ...\tau_k\}$ – это подмножество задач, для которых нагрузка u_i удовлетворяет неравенству:

$$u_i > \frac{n}{3n-2},$$

где n – число процессоров, которые участвуют в решении задач.

2. Младшие задачи $\{\tau_{k+1}, \tau_{k+2}, ..., \tau_n\}$ – это подмножество задач с нагрузкой:

$$u_i \le \frac{n}{3n-2}.$$

Любая из старших задач имеет более высокий приоритет по сравнению с любой из младших задач. Между старшими задачами приоритеты распределяются произвольно. Между младшими задачами приоритеты распределяются по убыванию частоты. Расстановка заданий по процессорам происходит во время выполнения набора задач планировщиком периода выполнения набора задач.

Среди методов планирования выполнения задач эти два метода являются наиболее широко используемыми. Каждый метод в отдельности из рассматриваемых методов может давать невыполнимые задачи. Для преодоления указанной трудности предлагается новая методика достижения выполнимости задач при расстановке задач по процессорам, используя эти две дисциплины планирования.

Сущность предлагаемой методики расстановки задач по процессорам. Для обеспечения выполнимости набора задач используется следующий критерий:

$$J = \max_i \max_j r_i^j . \qquad (1)$$

Рассмотрены две дисциплины планирования, сохраняющие приоритет задач и позволяющие экономить ресурсы компьютеров, а именно RM-планирование и RM_US-планирование, последовательно.

Создана компьютерная программа, которая расставляет задания по процессорам с помощью планировщика задач и моделирует процесс выполнения набора данных.

Разработанная методика включает следующие этапы:

1. *Планирование RM-метода*. Вначале используется метод RM-планирования. Для метода RM-планирования разработан планировщик периода разработки набора задач, загружающий очередной процессор задачами, пока не превышен его ресурс, и потом загружающий следующий процессор, и так далее. Берутся задачи из начала списка задач и дополняются задачами из конца списка задач для более полной загрузки процессора. Данные по задачам (период, время выполнения, оставшееся время выполнения задания, номер обрабатывающего процессора) хранятся в структуре данных «Задача».

2. *Планирование RM_US-метода.* Для метода RM_US-планирования расстановка заданий по процессорам происходит во время выполнения задач, и действует планировщик набора задач периода выполнения. Сначала задания расставляются по свободным процессорам, затем планировщик смотрит, превышает ли приоритет задания, выполняющегося на очередном процессоре, приоритет вновь пришедшего задания, и если да, то задание вытесняется с процессора,

определяется оставшееся время обработки вытесненного задания, и оно размещается в очереди заданий, поступивших на этот процессор согласно своему приоритету. Процессор начинает выполнять вновь пришедшее задание. Если свободных процессоров нет, и вытеснение заданий невозможно, задание помещается в наиболее короткую из очередей процессоров согласно своему приоритету. Данные по заданиям (оставшееся время выполнения задания, номер обрабатывающего процессора) хранятся в структуре данных «Задание».

3. *Проверка применимости рассматриваемых методов.* Моделируется выполнение набора задач для обоих методов планирования. Если имела место выполнимость задач в обоих случаях, критерием выбора метода планирования является наименьшее максимальное значение времени отклика для всех задач, согласно критерию (1) для метода RM-планирования и метода RM_US-планирования.

4. *Решение о выборе метода планирования.* Если выполнимость задач имела место только в одном случае, выбирался этот вариант планирования набора задач. Если выполнимость набора задач не достигалась ни в одном из случаев, выбирается метод RM-планирования, для которого выполняется корректировка расстановки задач по процессорам с возможным добавлением одного или даже нескольких процессоров.

Программная система имеет интерфейс, состоящий из нескольких окон для удобства ввода информации и оценки полученных данных.

Иллюстрирующий пример. Рассмотрим набор из пяти задач (рисунки 1,2,3), который должен выполняться по оценке программной системы на трех процессорах. На рисунке 1 представлено главное окно программы. Для пользования программой вводятся число задач, средняя производительность системы в долях единицы для оценки числа требуемых процессоров, время замещения задачи более приоритетной задачей в процентах от минимальной задачи, которая может выполняться на процессорах и время моделирования в микросекундах.

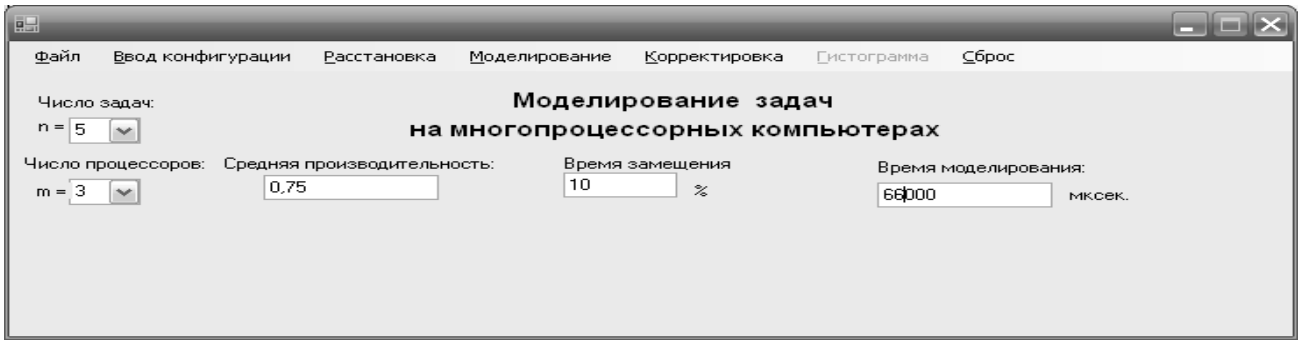


Рис. 1. Главное окно программы

Данные для примера генерировались с помощью генератора случайных чисел по равномерному закону распределения.

Время моделирования рассчитывается как произведение всех значений периодов с учетом кратности. Тогда набор заданий вернется в изначальное состояние – все задания выстроятся в очереди на выполнение. Чтобы уменьшить период моделирования, сгенерированные значения округляются в большую сторону. Для данного набора задач минимальный период моделирования равен $500 \times 12 \times 11$=66000 мкс.

По результатам моделирования выполнения наборов задач строятся следующие таблицы:

- рисунок 2 – таблица для RM_US-планирования;
- рисунок 3 – таблица для RM-планирования.

На рисунке 2 приведена таблица, полученная для RM_US-планирования. Номер процессора задачи и его нагрузка не заданы, потому что они определяются на шаге выполнения задач во время моделирования.

В таблицах обозначено:T – период задачи,C – время выполнения задачи, U – нагрузка задачи, P – приоритет задачи, Rmin – минимальное значение времени отказа, Rmax – максимальное значение времени отказа, Nproc – номер процессора, на котором решается задача, PProc – суммарная нагрузка этого процессора, Rmd1 – среднее арифметическое время отказа, Rmd2 – среднее время отказа, считающееся вторым способом.

Значения всех временных характеристик приведены в микросекундах.

На рисунке 3 приведена таблица, полученная для RM-планирования. Из этой таблицы видно, что заданы номер процессора задачи и его нагрузка. Видно также, что при RM-US-планировании меньше минимальный и максимальный отклик для четвертой и пятой задачи, а также среднее значение отклика, подсчитанное двумя способами: одно среднее арифметическое и второе получается сложением каждого следующего значения отклика и делением на два. Отметим, что оба набора данных выполнимы на данном наборе процессоров.

Таблица

Число процессоров 8 Конфигурация 5 задач Суммарная про

	T:	C:	U:	P:	Rmin:	Rmax:	Nproc:	Pproc:	Rmd1:	Rmd2:
01	500	280	0,56	1	280	280	0	0	280	280
02	1200	640	0,53333	1	640	640	0	0	640	640
03	300	100	0,33333	2	100	100	0	0	100	100
04	400	170	0,425	3	170	270	0	0	188,666	171,585
05	1100	340	0,30909	4	340	900,25	0	0	604,645	590,481
06	-	-	-	-	-	-	-	-	-	-
07	-	-	-	-	-	-	-	-	-	-
08	-	-	-	-	-	-	-	-	-	-
09	-	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-	-

Рис. 2. Таблица для RM_US-планирования

Из таблиц видно, что времена отклика не всегда являются целыми числами, хотя время выполнения задач и их период целочисленные. Дело в том, что при замещении задания расходуется процессорное время на снятие менее приоритетной и постановки более приоритетной задачи на процессор. Это время рассчитывается как 10% от задачи минимальной продолжительности в 50 команд по пять тактов на команду. Если тактовая частота процессора равняется примерно 100 МГц, тогда задержка на замещение задачи составит примерно 0,25 микросекунд, что легко получается из составленной пропорции.

Таблица

Число процессоров 8 Конфигурация 5 задач Суммарная про

	T:	C:	U:	P:	Rmin:	Rmax:	Nproc:	Pproc:	Rmd1:	Rmd2:
01	300	100	0,33333	1	100	100	2	0,86666	100	100
02	400	170	0,425	1	170	170	3	0,425	170	170
03	500	280	0,56	1	280	280	1	0,86909	280	280
04	1100	340	0,30909	2	620,099	900,200	1	0,86909	784,119	795,635
05	1200	640	0,53333	2	1040,3	1040,3	2	0,86666	1040,3	1040,3
06	-	-	-	-	-	-	-	-	-	-
07	-	-	-	-	-	-	-	-	-	-
08	-	-	-	-	-	-	-	-	-	-
09	-	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-	-

Рис. 3. Таблица для RM-планирования

Таким образом, видно, что метод планирования RM_US является более эффективным в смысле выбранной методики.

Заключение. Рассмотрены методы планирования: RM-метод и RM_US-метод. Установлено, что ни один из данных методов не обеспечивает в общем случае надлежащей выполнимости набора задач. Предложена новая методика планирования загрузки процессоров для систем реального времени. Разработанная методика позволяет выбрать рациональный метод планирования загрузки процессоров по времени отклика, что приводит к увеличению фактической производительности процессоров при решении конкретных задач и обеспечивает выполнимость всего набора задач. В рассматриваемом примере выигрыш при применении метода RM_US-планирования составляет 13% процессорного времени. Работоспособность методики проверена на ряде примеров. Показано, что для выполнимости набора задач следует применять совокупность рассмотренных методов планирования в строго определенной последовательности. Это дает возможность выполнять наборы задач, которые не могут обслуживаться ни одним из этих методов в отдельности. Приводится тестовый результат.

СПИСОК ЛИТЕРАТУРЫ

1. Никифоров В.В. Выполнимость приложений реального времени на многоядерных процессорах – СПб.: Труды СПИИРАН(8), 2009, С.255–284.
2. Liu C., Layland J. Scheduling Algorithms for Multiprocessing in a Hard Real-Time Environment – Journal of the ACM, 1973. vol. 20. no. 1. pp.46–61.
3. Dhall S.K, Liu C. On a Real-Time Sheduling Problem – Operating Research, 1978. vol. 26, no. 1, pp.127–140.
4. Anderson B., Daruah S., Jonson J. Static-Priority Scheduling on Microprocessors – Proceedings of 22 IEEE Real-Time Systems Symposium, 2001. pp.193–202.
5. Anderson B. Static-Priority Scheduling on Microprocessors – Thesis for the degree of Doctor of Philosophy, Chalmers University of Technology, Geteborg, 2003. P.129.
6. Srinivasan A., Anderson J. Early-Reliase Fair Scheduling – Procs of the 12-th Euromicro Conference on Real-Time Systems. 2000. P.35–43.
7. Докучаев А.Н. Особенности диспетчеризации сверхлегких задач в мультипроцессорных и вычислительных системах – СПб.: Информационные технологии, 2012. №2, С.14–17.
8. Калачева С.Б. Анализ двух методов планирования расстановки задач для систем реального времени с использованием нескольких процессоров – СПб.: «РИ–2012», 2013. С.100–103.

УДК 681.3.06

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ СИСТЕМАТИЗАЦИИ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОГО ВЫБОРА НА КОНЕЧНОМ МНОЖЕСТВЕ АЛЬТЕРНАТИВ[2]

Микони Станислав Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., д. 39,
e-mail:smikoni@mail.ru

Аннотация: Сформулированы аксиомы, позволившие установить сходство и различие известных методов многокритериального выбора на конечном множестве альтернатив. Показаны связи между методами, объединившие их в систему. Изложенная теория положена в основу учебника «Теория принятия управленческих решений».

Ключевые слова: *аксиома; шкала; целевое значение признака; критерий оптимизации; функция полезности*

THEORETICAL JUSTIFICATION OF SYSTEMATIZATION OF METHODS MULTICRITERIA OPTIMIZATION ON A FINITE SET OF ALTERNATIVES [1]

Stanislav Mikoni
St. Petersburg Institute for Informatics and Automation
of the Russian Academy of Sciences
SPIIRAS, 39, 14-th Line V.O., St. Petersburg, Russia,
e-mail: smikoni@mail.ru

Abstract: Formulated axioms, which allowed to establish similarities and differences between the known methods of multi-criteria selection on a finite set of alternatives. Showing links uniting methods in the system. The theory is the basis of the textbook "The theory of management decision-making".

Keywords: *axiom; scale; target feature; criterion; utility function*

Введение. В современной истории можно выделить три этапа изучения моделей и методов принятия решений.

На первом этапе решались, в основном, оптимизационные задачи преимущественно на континуальном множестве альтернатив. Эта область принятия решений получила развитие в связи с необходимостью получения экономического эффекта в промышленных и транспортных технологиях и военного эффекта в боевых операциях. Массовый характер и тех и других стимулировал интерес промышленников и военных к решению этой проблемы, а учёных – к поиску методов решения оптимизационных задач. В рамках научного направления «Исследование операций» были разработаны модели математического программирования и теории игр и реализующие их оптимизационные пакеты программ.

Второй этап связан с бурным развитием вычислительной техники во второй половине XX века. Развитие теории принятия решений стимулировала разработка информационно-советующих систем, входивших в состав автоматизированных систем управления (АСУ). При решении проблемы человеко-машинного взаимодействия большое внимание было уделено роли человеческого фактора, что стимулировало развитие экспертных методов. Возросшая доля человеческого фактора в моделях и методах принятия решений способствовала их выделению из дисциплины исследования операций и объединению в качестве теории принятия решений с научным направлением «Искусственный интеллект». Разработанные в его рамках методы воплощались в экспертные системы оценивания, информационно-советующие и экспертные системы.

Третий этап связан с развитием информационного общества в конце XX века, в котором информатика проникла во все сферы человеческого бытия. Это способствовало автоматизации решений на всех уровнях управления в рамках разработки СППР (систем поддержки принятия решений). В исследованиях стало уделяться большое внимание формализации различных видов неопределённости, присутствующей как в исходных данных, так и в предпочтениях лица, принимающего решение (ЛПР).

Современные учебные пособия по теории принятия решений можно разделить на три категории. Первая из них [1], [2] охватывает модели и методы выбора, разработанные на всех этапах развития теории принятия решений. Специализированные пособия ориентированы либо на метод [3], либо на экономику, либо на то и другое [4]. К третьей категории отнесём учебные пособия по методам принятия управленческих решений [5].

[2] Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00439)

Каждой из этих категорий учебников присущи свои недостатки. Первая категория в силу разно плановости методов не рассчитана на практическое применение в управленческих задачах. Учебные пособия второй группы рассчитаны на усвоение ограниченного количества методов. Учебные пособия по методам принятия управленческих решений ориентированы на широкий класс задач предпринимательской деятельности, понимаемой как менеджмент.

Между тем, не все управленцы являются предпринимателями, а круг решаемых ими задач не ограничивается получением прибыли. В любой сфере деятельности (производственной, образовательной, научной, культурной, социальной и пр.) лицо, принимающее решение (ЛПР), решает такие задачи, как:

1) определение варианта организационной структуры;
2) подбор работников;
3) распределение задач между отдельными подразделениями или работниками;
4) установление взаимодействия между подразделениями или работниками;
5) определение порядка и времени проведения работ.

Функция руководства организацией предусматривает решение таких задач как:

1) текущий контроль деятельности сотрудников;
2) распределение вознаграждения по результатам работы;
3) поощрение лучших работников.

Контроль деятельности организации осуществляется по итогам её функционирования за конкретный период (месяц, квартал, год, пятилетку):

1) определение лучших подразделений или работников;
2) определение узких звеньев.

Все перечисленные задачи являются, как правило, многокритериальными, а область их определения не превышает нескольких десятков альтернатив. Главным отличием этих задач от задач, решаемых методами исследования операций, является необходимость непосредственного участия ЛПР в проектировании модели выбора. Предпочтения ЛПР должны быть учтены как при формулировании частных целей в процессе построения дерева целей, так и при задании их важности. Именно объём участия ЛПР в проектировании модели выбора резонно принять за признак, выделяющий организационные управленческие решения от других задач принятия решений в сфере управления. Но для создания теории принятия управленческих решений этого недостаточно. Необходимо подвести общую теоретическую базу под все методы многокритериального выбора, применяемые для формализации управленческих операций. Решению этой задачи посвящена данная работа.

1. Методы многокритериального выбора. Методы многокритериальной оптимизации и классификации рассчитаны на упорядочение объектов (альтернатив, вариантов) по многим признакам или отнесение их к упорядоченным по качеству классам. Методы оптимизации делятся на следующие группы:

1. Векторная оптимизация (Dominance analysis);
2. Скалярная оптимизация (Multiobjective optimization);
3. Многоатрибутная оптимизация по полезности (Utility-based multiattribute optimization);
4. Вычисление приоритетов на основе парных сравнений (Pairwise prioritization).

Методы классификации (Multicriteria classification) используют либо нечёткие классы, либо группируются по близости многокритериальных оценок.

Каждая группа включает несколько методов. К методам векторной оптимизации относятся:

1. упорядочение на основе отношения Парето-доминирования;
2. лексиминная оптимизация [6];
3. лексикографическая оптимизация;
4. оптимизация на основе единой шкалы изменения качества (ЕШИК) [7].

К методам скалярной оптимизации относятся:

1. оптимизация по достижению цели;
2. условная оптимизация;
3. оптимизация по отклонениям от цели;
4. оптимизация по индивидуальным целям.

Каждый метод имеет свои разновидности. Например, методы скалярной оптимизации могут различаться обобщающими функциями, а методы теории полезности различаются способом создания функций (лотереей, оценкой ценности и т.п.).

В соответствии со своими именами все перечисленные методы решают задачу оптимизации. Это относится и к задачам классификации с упорядоченными по качеству классами. Объект, отнесённый к классу «Высокое качество» (ВК), безусловно, *лучше* по качеству объекта, отнесённого к классу «Среднее качество» (СК). Применительно к задачам многокритериальной оптимизации на конечном множестве альтернатив следует использовать именно термин «лучший», а не «оптимальный», как в классических задачах оптимизации. Это объясняется отсутствием строгого доказательства оптимального решения в условиях неопределённости предпочтений ЛПР и эвристической природы способов их обработки.

Перечисленные методы многокритериального выбора разрабатывались, как правило, изолированно друг от друга, и каждый из них имеет свою аксиоматику. Сведение их в систему требует создания общей аксиоматики. Рассмотрим понятия, участвующие в аксиоматизации.

2. Основные понятия многокритериального выбора. К основным понятиям, применяемым при решении задачи многокритериального выбора и представленным на рисунке 1, относятся: признак f_j объекта x_i, полезность j-го признака $u(y_j)$, шкалы признака и полезности, целевое значение признака (цель оптимизации), идеальная и реальная цели, предпочтения на шкалах, критерий оптимизации, функция полезности. Все понятия объединены относительно графика функции полезности, кусочно-линейной или нелинейной.

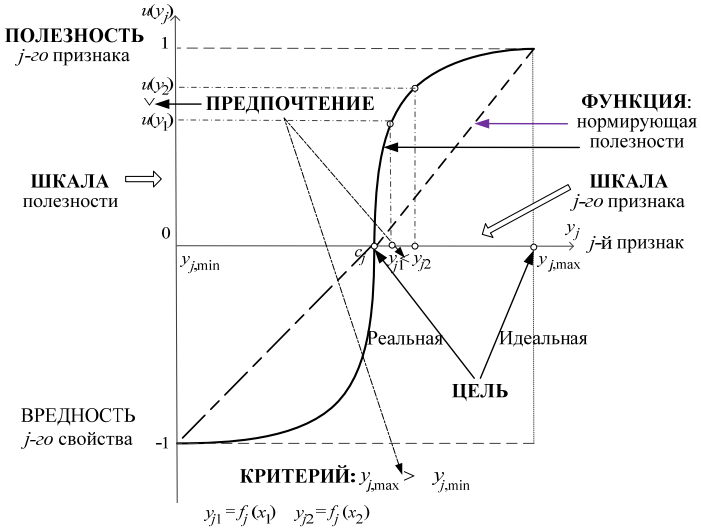


Рис.1. Основные понятия многокритериального выбора

Признак f_j отражает j-е свойство оцениваемого объекта x_i. Объект x_i может оцениваться как в шкале признака [$y_{j,\min}, y_{j,\max}$], так и в шкале полезности/вредности [–1, +1]. Полуось [–1, 0] «Вредность» используется для отражения потерь ЛПР. Если в задаче выбора потери отсутствуют, то используется только полуось полезности [0, +1].

Под идеальной понимается цель (*целевое* значение признака) c_j, совпадающая с одной из границ шкалы $[y_{j,\min}, y_{j,\max}]$: $c_j = y_{j,\max}$ или $c_j = y_{j,\min}$. Под реальной понимается цель c_j, не совпадающая с границей шкалы: $y_{j,\min} < c_j < y_{j,\max}$.

Двухместное отношение предпочтения описывается предикатом превосходства $\succ$ $f_j(x_i)$, $f_j(x_k)$ с $f_j(x_k)$ в роли базы сравнения. Здесь $y_i = f_j(x_i)$, $y_k = f_j(x_k)$ – значения признака для объектов x_i и x_k. Предпочтение $\succ (y_{j,\min}, c_j)$ называется критерием оптимизации на шкале j-го признака, целевым – при $c_j = y_{j,\min}$ $(c_j = y_{j,\max})$ и ограничительным – при $y_{j,\min} < c_j < y_{j,\max}$.

Предикат предпочтения $Pr \geq (f_j(x), c_j)$ делится на предикаты:

– превосходства $Pr > (f_j(x), c_j)$, $Pr < (f_j(x), c_j)$;

– соответствия $Pr = (f_j(x), c_j)$, $Pr_{][}(f_j(x), c_{j,H}, c_{j,B})$.

Под функцией полезности понимается отображение $u: Y \to$ [0, 1]. На рисунке 1 приведены линейная и нелинейная функции полезности.

3. Аксиомы методов многокритериального выбора на конечном множестве альтернатив.

Очевидным способом формирования аксиом, как основополагающих положений общей теории многокритериального выбора на конечном множестве альтернатив, является исключение особенностей методов, что позволяет группировать их в классы. Исключённые особенности используются в качестве видовых отличий методов, связующих их между собой. Перечислим основополагающие положения, обеспечивающие сходство рассматриваемых методов.

1. Оценивание объекта *x* по многим критериям выполняется либо в шкалах этих критериев, либо в общей шкале [0, 1] или [–1, +1].

2. Целевое значение c_j j-го признака может быть *любым* в пределах шкалы $[y_{j,\min}, y_{j,\max}]$: $y_{j,\min} \le c_j \le y_{j,\max}$. Это положение позволяет устранить различие между целевым и ограничительным критерием и использовать их как совместно, так и в качестве видовых отличий.

3. Предикат превосходства и соответствия обобщаются в предикат предпочтения $Pr \ge (f_j(x), c_j)$, который представляется *оценочной функцией* $p_j : Y_j * C \to$ [0, 1]. Шкала [0, 1] является бесконечнозначным обобщением двоичного предиката {0, 1}, что позволяет использовать для оценки истинности нечёткую логику.

4. Значение предиката $p_j < 1$ трактуется как *частичное достижение* цели c_j. Частичное достижение цели c_j объектом x не является поводом для его *исключения из оценивания*. Это позволяет включить метод условной оптимизации с отсеиванием альтернатив в группу методов многокритериального выбора, оценивающих, в том числе, альтернативы с частичным достижением целей.

5. Любое отображение $\delta_j : Y_j \to$ [0, 1] значения $y_j = f_j(x)$ j-го признака в шкалу [0, 1] принимается за *функцию полезности* $u_j : Y_j \to$ [0, 1] независимо от способа её создания. Это позволяет рассматривать нормирующие функции и функции ценности как частные случаи функции полезности.

6. На основе ограничительных критериев «не менее» и «не более» создаются монотонные функции полезности, а на основе критериев «равно» и «интервал» – немонотонные функции полезности. И те, и другие являются кусочно-линейными при нормировании участков шкалы признака, либо нелинейными – при задании предпочтений на участках шкалы.

7. Отображение разности $f_j(x) - c_j$ в шкалу [–1, 1] принимается за *функцию отклонения от цели* $\gamma_j : \Delta C_j \to$ [–1, 1]. Это позволяет учитывать как невыполнение, так и перевыполнение цели, как в отдельности, так и в совокупности.

8. Обобщением шкалы [–1, 0, 1] является процентная шкала [0%, 100%, 200%]. Измерение меры невыполнения и перевыполнения плановых заданий позволяет сопоставлять объекты с разными ресурсами по степени выполнения ими индивидуальных плановых заданий.

4. Систематизация методов на основе общей аксиоматики. Согласно аксиоме 1 все методы делятся на две группы. К первой группе относятся методы, не требующие общей шкалы для оценивания объекта x. Они используют шкалы критериев и на этом основании называются методами критериального выбора. Использование всех критериев методами этой группы для установления линейного порядка на конечном множестве альтернатив основано на сквозном упорядочении их значений. Лексикографическая оптимизация использует с этой целью приоритет критериев, а методы вербального анализа решений (ВАР) – единую шкалу изменения качества (ЕШИК). Эти методы различаются между собой детальностью предпочтений. В то время как в лексикографической оптимизации предпочтения задаются на множестве критериев, в методах ВАР они задаются на множестве пар значений всех критериев. Очевидно, что такое увеличение трудоёмкости создания модели ВАР окупается большим доверием к результатам выбора.

У двух других методов векторной оптимизации отсутствуют предпочтения на множестве критериев, что позволяет устанавливать этими методами только частичный порядок множестве объектов. В силу упорядочения векторной оценки каждого объекта по качеству лексиминная оптимизация обеспечивает большую строгость порядка по сравнению с упорядочением на основе отношения Парето-доминирования. Графическое представление системы методами критериального выбора приведено в [8].

Методы второй группы используют единую шкалу для вычисления общей оценки объектов по всем признакам. Единая шкала требуется для обобщения частных оценок, измеренных в разных шкалах. Как правило, обобщённые оценки вычисляются с применением усредняющих функций, которые векторной оценке объекта ставят в соответствие число (скаляр). Для преобразования шкал признаков в единую шкалу используются различные функции. Независимо от вида функций использующие их методы назовём методами функционального выбора.

Согласно аксиоме пятой все функции, отображающие значения шкалы признака в единую шкалу [–1, 0, 1] или [0, 1], принимаются за функции полезности. Согласно аксиоме семь функция, отображающая разность $f_j(x)$ – c_j в шкалу [–1, 1] принимается за функцию отклонения от цели. Таким образом, в зависимости от отношения к цели методы функционального выбора делятся на две группы – по достижению цели и отклонению от цели.

Методы достижения цели различаются по способу создания функций полезности – вычисляемых и задаваемых экспертами. К вычисляемым функциям относятся нормирующие функции критериев и функции приоритетов в матрицах парных сравнений. Более подробно все функции

полезности рассмотрены в [9]. Методы многокритериальной оптимизации, использующие линейные нормирующие функции критериев, назовём методами достижения идеальной цели (ДИЦ). Методы многокритериальной оптимизации с ограничениями, использующие кусочно-линейные нормирующие функции с перегибом в точке c_j, $j=\overline{1,n}$, назовём методами достижения реальной цели (ДРЦ). Функции приоритетов используются методом анализа иерархий (МАИ).

Функции, задаваемые экспертами, разделим на две группы – по предпочтениям экспертов и плановым заданиям. К первой группе относятся нелинейные функции, определяемые на основе лотерей (риска ЛПР) и функции ценности. Их реализует метод многоатрибутной оптимизации по полезности (МОП). Функции, отражающие плановые задания, использует метод оптимизации по индивидуальным целям (ОИЦ).

В группу методов отклонения от цели входят методы условной оптимизации (УО) и оптимизации по отклонению от цели (ООЦ). Первый из них отсеивает объекты, не удовлетворяющие ограничению хотя бы по одному критерию. Методы оптимизации по отклонению от цели оценивают объекты по всем критериям. Невыполнение ограничения как цели оценивается штрафом, а перевыполнение цели – поощрением (бонусом). Это позволяет вычислять три вида обобщённых оценок: только по штрафам, только по поощрениям и по алгебраической сумме штрафов и поощрений. Графически взаимосвязь методов функционального выбора (МФВ) представлена на рисунке 2. Подчёркнуты основания деления методов (системообразующие признаки). Курсивом представлены видовые отличия (значения признаков). В правом столбце помещены основные методы функционального выбора.

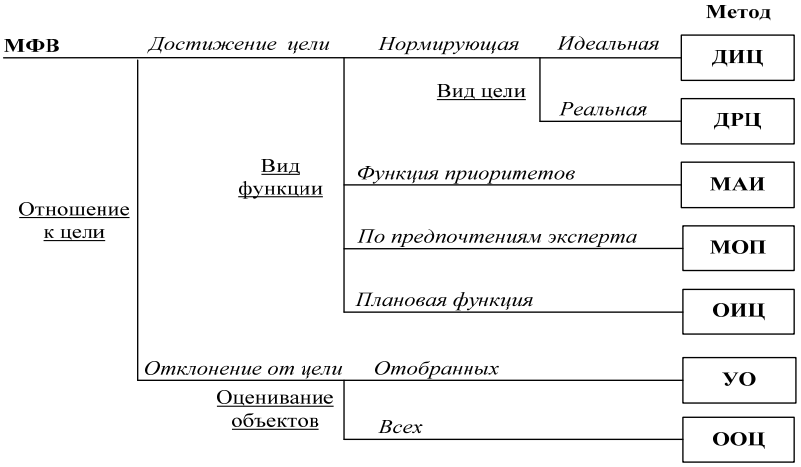


Рис.2. Классификация методов функционального выбора

Заключение. Исследователи, предлагающие свои методы решения проблемы, обычно не озабочены встраиванием их в общую систему. Более того, они заинтересованы подчёркивать отличие своего метода от существующих. Между тем, очевидно, что методы, нацеленные на решение общей проблемы, должны иметь сходство. Именно, оно позволяет объединить изначально изолированные сущности в систему. Сходство выявляется путём исключения частных ограничений метода с целью перехода к общим ограничениям, присущим всем методам решения одной проблемы.

Предложенная в работе группа аксиом имеет отношение, в той или иной степени, ко всем методам выбора. Это позволяет рассматривать её в качестве базовой характеристики всех методов выбора. Частные особенности методов рассматриваются в качестве видовых отличий. Обнаруженное через аксиомы сходство и различие методов даёт теоретическое обоснование системы методов, что важно для их изучения и определения сферы эффективного применения. Изложенная теория была положена в основу учебника «Теория принятия управленческих решений» [9].

СПИСОК ЛИТЕРАТУРЫ

1. Черноруцкий И.Г. Методы принятия решений. Учебное пособие. –СПб.: БХВ-Петербург, 2005. Петровский А.Б. Теория принятия решений. Университетский учебник. –М.: ИЦ «Академия», 2009. –408 с.
2. Петровский А.Б. Теория принятия решений. Университетский учебник. –М.: ИЦ «Академия», 2009. –391 с.
3. Саати Т.Л. Принятие решений при зависимостях и обратных связях.–М.: Изд-во ЛКИ, 2007. –357 с.
4. Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. –М.: Финансы и статистика, 2004. –464 с.
5. Литвак Б.Г. Управленческие решения. Практикум. - М.: Московская Финансово-Промышленная Академия, 2012. –448 с.
6. Подиновский В.В. Введение в теорию важности критериев в многокритериальных задачах принятия решений. –М.: Физматлит, 2007, 37 с.
7. Ларичев О.И. Вербальный анализ решений.– М.: Наука, 2006. –181 с.
8. Микони С.В. Системный анализ методов многокритериальной оптимизации на конечном множестве альтернатив // Труды СПИИРАН, 2015, выпуск 4(41), Стр. 180–199.
9. Микони С.В. Теория принятия управленческих решений. Учебное пособие. –СПб.: Лань 2015. –448 с.

УДК 004.4

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИСПОЛНЕНИЯ ПРОГРАММНЫХ КОМПЛЕКСОВ ДЛЯ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Никифоров Виктор Викентьевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия В.О., д. 39,
e-mail: nik@iias.spb.su

Аннотация: Изложен подход к построению комплекса программных средств для имитационного моделирования работы систем реального времени. Входные данные для работы моделирующего комплекса включают модельные описания каждой из задач моделируемой системы: значение периода активизации задачи, особенности внутренней структуры кода задачи. Код каждой из моделируемых задач представляется линейной последовательностью сегментов. Каждый сегмент кода задачи представляет собой отрезок кода, заключенный между двумя соседними системными операторами: начало кода задачи, запрос системного ресурса, освобождение системного ресурса, завершение задачи. Для каждого сегмента указывается объем процессорного времени, требуемого для его исполнения. Выходные данные моделирующего комплекса включают последовательность системных событий, возникающих в ходе имитационного моделирования (с указанием соответствующих им значений модельного времени) и необходимые производные параметры.

Ключевые слова*: системы реального времени, статические модели многозадачных приложений, выполнимость задач, имитационное моделирование многозадачных приложений.*

SIMULATION OF SOFTWARE APPLICATION EXECUTION IN REAL-TIME SYSTEMS

Victor Nikiforov
St.Petersburg Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line, 39,
e-mail: nik@iias.spb.su

Abstract: An approach is proposed for building of software tool that serves for simulation of software application execution in real-time systems. The input data of simulator tool includes the static model descriptions for each task in simulated software application: first - the value of task activation period, second - the peculiarity of task code internal structure. Any application task code is supposed to be the liner sequence of code sections. Every code section is the code interval between two neighbor system operations: task start point, request for a system resource, free a system resource and task end point. The amount of processor time for execution of each task section is also included as input data of simulator. The output data of the simulator tool contains the sequence of system events that occur during simulation (with corresponding values of modeling time) and the required derivative data.

Keywords: *real-time systems, static models of multitask applications, task feasibility, simulation of execution of real-time systems applications.*

Введение. Программное приложение для систем реального времени (СРВ) как правило, строится в виде комплекса кооперативных (действующих для достижения общих стоящих перед системой целей) *задач* τ_1, τ_2, … τ_n, [1]. Очередная, j-я активизация задачи τ_i означает порождение очередного, j-го ее экземпляра – порождение *задания* ${}_j\tau_i$. Отличительной особенностью СРВ является требование своевременности выполнения задач, которое выражается в том, что продолжительность интервала существования любого экземпляра ${}_j\tau_i$ задачи τ_i не должна превышать предельного значения D_i [2]. При введении понятия *время отклика* задачи $R_i = \max\{{}_1\tau_i, {}_2\tau_i, ...\}$ требование своевременности выражается неравенством $R_i \le D_i$ [3]. Под выполнимостью многозадачного программного приложения для СРВ, понимается его свойство, состоящее в том, что при любом допустимом сценарии системных событий обеспечивается справедливость неравенства $R_i \le D_i$ для каждой из задач τ_i. Для проверки выполнимости программного приложения строятся и анализируются структурные модели задач, выполняются оценки времени отклика для каждой из задач с учетом факторов, влияющих на значения R_i.

Одним из универсальных инструментов проверки выполнимости программных приложений реального времени является применение технологии имитационного моделирования. Представляемый ниже подход к построению системы имитационного моделирования работы

многозадачного программного комплекса излагается на упрощенном примере моделирования системы из независимых задач (задач без синхронизирующих межзадачных интерфейсов), применяющей дисциплину планирования со статическими приоритетами задач. Однако, состав объектов и процедур, обеспечивающих функционирование упрощенного моделирующего комплекса программ, может быть естественным образом модифицирован и дополнен для моделирования работы систем с произвольными дисциплинами планирования и с разделением информационных ресурсов под произвольными протоколами доступа.

1. Исходные данные для процесса моделирования. Представляемая архитектура программного комплекса для имитационного моделирования опирается на использование трех цепных списков:

`TaskList` – список дескрипторов задач;

`ReadyList` – список активных заданий;

`EventList` – список запланированных системных событий.

Исходными данными для процесса имитационного моделирования является перечень TaskList дескрипторов задач, составляющих моделируемое программное приложение. Каждая из задач характеризуется тремя параметрами:

`Period` – длина интервала времени между соседними моментами активизации;

`C_size` – объем процессорного времени, необходимый для выполнения;

`Piority` – целое число, определяющее приоритет.

Состав задач и значения перечисленных параметров остаются неизменными в рамках сеанса моделирования.

Все объекты, связываемые в списки `TaskList`, `ReadyList`, `EventList` принадлежат классам, являющимся наследниками класса `ListNode`:

```
class ListNode {
  ListNode *Next;
  ListNode* Pop(){
    ListNode *ret_ptr = Next;
    if(ret_ptr != 0) Next = ret_ptr->Next;
    return(ret_ptr);
  }
  void Push(ListNode *chain){
    if(chain != 0) {
      chain->Next = Next;
      Next = chain;
    }
  }
}
```

Метод `Push(ListNode *chain)` позволяет вставлять в список новое звено `chain`; метод `Pop( )` обеспечивает выполнение обратной операции — удаление звена из списка. Совместное использование этих методов позволяет осуществить модификацию списка в режиме LIFO-буферизации.

Ближайшим наследником класса `ListNode` является класс `OrderedNode`, используемый для построения списков объектов, упорядоченных по значению специального атрибута `Ordering`:

```
class OrderedNode:ListNode {
  int Ordering;
  OrderedNode* Find(int key) {
    OrderedNode *suc_ptr;
    ListNode *pre_ptr = this;
    while((suc_ptr = (OrderedNode *)
                  pre_ptr->Next) != 0) {
      if(suc_ptr->Ordering >= key) break;
      pre_ptr = suc_ptr;
    }
    return(pre_ptr);
  }
}
```

Метод `Find(int key)` обеспечивает поиск в списке места, соответствующего значению ключа key. Назначением упорядоченных списков, содержащих объекты класса `OrderedNode`, является, в частности, упорядочение (по приоритету) объектов, выступающих в качестве дескрипторов задач в списке `TaskList`.

Дескриптор каждой задачи является объектом класса Task. Класс Task является непосредственным наследником класса OrderedNode (и, соответственно, опосредованным наследником класса ListNode):

```
class Task:OrderedNode {
   int Period;
   int C_size;
   int R_time;
}
```

Дополнительно к атрибутам класса OrderedNode дескриптор задачи имеет атрибуты Period и C_size для представления соответствующих параметров задач каждой из задач. Атрибут R_time используется для представления результата моделирования: максимального времени отклика задачи.

Дескрипторы задач генерируются и размещаются в списке TaskList (с упорядочением по приоритетам) в ходе выполнения процедуры TaskBuild(), которая обеспечивает построение дескрипторов задач либо в диалоге с пользователем, либо в ходе выполнения специальной генерирующей программы.

Дескрипторы задач связываются в цепной список TaskList за счет использования атрибута Next, унаследованного от класса ListNode. Упорядочение дескрипторов задач по приоритетам выполняется за счет использования атрибута Ordering, унаследованного от класса OrderedNode.

2. Динамически модифицируемые списки. Список задач TaskList формируется при подготовке к выполнению моделирования и остается неизменным в ходе выполнения сеанса моделирования. Списки ReadyList и EventList. формируются при инициализации сеанса моделирования и модифицируются в ходе выполнения сеанса.

Список ReadyList дескрипторов заданий содержит объекты класса Job:

```
class Job:OrderedNode {
   int Start_time;
   int Rest_C_size;
   Task *Job_class;
}
```

Содержащиеся в списке ReadyList объекты моделируют активные в текущий момент модельного времени задания – задания, претендующие на ресурс процессора. Атрибут Start_time объекта класса Job фиксирует момент модельного времени порождения этого объекта. Атрибут Rest_C_size указывает ту часть объема процессорного времени, которая еще не израсходована заданием. Атрибут Job_class связывает дескриптор задания с соответствующим ему дескриптором задачи.

Дескрипторы заданий связаны в цепной список за счет использования атрибута Next, унаследованного от класса ListNode и упорядочены в этом списке по значению атрибута Ordering, унаследованного от класса OrderedNode. Особое место занимает дескриптор задания, размещенный в самом начале списка ReadyList (дескриптор, возглавляющий список ReadyList). Этот дескриптор называется дескриптором текущего задания.

Список EventList содержит дескрипторы системных событий – объекты класса Event:

```
class Event:OrderedNode {
   int Event_type;
   Task *Task_ptr;
   Job *Job_ptr;
}
```

Атрибут Event_type принимает одно из двух значений – ноль (если событие состоит в активизации задачи, указываемой атрибутом Task_ptr) или единица (если событие состоит в завершении задания, указываемого атрибутом Job_ptr).

Унаследованный от класса OrderedNode атрибут Ordering, указывает соответствующий событию момент модельного времени (в списке EventList дескрипторы системных событий упорядочены по этому атрибуту). Связывание дескрипторов системных событий в цепной список выполняется за счет использования системного атрибута Next, унаследованного от класса ListNode.

3. Инициализация процесса моделирования. Глобально доступные объекты TaskList, ReadyList и EventList класса ListNode генерируются статически со значениями атрибута Next равными NULL. Кроме того, генерируются глобальные переменные

```
int cur_time = 0;
context_switchs = 0;
```

Переменная cur_time используется для отслеживания течения модельного времени. Максимально допустимое значение этой переменной задается константой TIME_LIMIT. Переменная context_switchs используется для подсчета числа переключений контекста.

В результате выполнения процедуры TaskBuild(), строится список задач TaskList, глобальная переменная task_number принимает соответствующее значение.

Для каждой из задач генерируется объект класса Event со значениями атрибутов:

```
Ordering = 0;
Event_type = 0;
Job_ptr = NULL;
```

Атрибут Task_ptr настраивается на указание дескриптора соответствующей задачи; атрибуты Next в произвольном порядке связывают генерируемые объекты класса Event в цепной список, начинающийся глобально доступным объектом EventList.

На этом инициализация процесса моделирования заканчивается, начинается пошаговая обработка дескрипторов системных событий из списка EventList.

4. Выполнение шага моделирования. На каждом шаге моделирования обрабатывается дескриптор системного события, размещенный в начале списка EventList (головной дескриптор списка). При обработке головного дескриптора системного события в первую очередь выполняются специфические действия очередного шага моделирования: в зависимости от значения атрибута Event_type головного дескриптора из списка EventList специфические действия состоят либо в выполнении процедуры активизации задачи, либо в выполнении процедуры завершения задания.

Активизация задачи. Если для головного дескриптора системного события Event_type = 0 (дескриптор предписывает активизацию задачи) то специфические действия состоят в том, что моделируется порождение очередного задания типа EventList.Next->Task_ptr. Для этого генерируется новый дескриптор задания со значениями атрибутов

```
Start_time = cur_time;
Job_class = EventList.Next->Task_ptr;
Ordering =
   EventList.Next->Job_class->Ordering;
Rest_C_size =
   EventList.Next->Job_class->C_size;
```

Дескриптор порожденного задания вставляется в список активных заданий ReadyList. Размещение дескриптора задания в ReadyList соответствует приоритету задания. Если в списке активных заданий размещаются задания с совпадающими значениями атрибута Ordering, то среди них более приоритетными считаются задания с меньшими значениями атрибута Start_time.

В список системных событий EventList вставляется новый объект типа Event со следующими значениями атрибутов:

```
Ordering = cur_time +
    ReadyList.Next->Task_ptr->Period;
Event_type = 0;
Job_ptr = NULL;
Task_ptr = ReadyList.Next->Task_ptr;
```

Размещение вновь порожденного дескриптора системного события в списке EventList определяется значением его атрибута Ordering.

Если при активизации задачи произошла смена текущего задания (изменилось значение атрибута ReadyList.Next), то значение глобальной переменной context_switchs, отслеживающей число переключений контекста, увеличивается на единицу.

Завершение задания. Если для головного дескриптора задания Event_type=1, то есть, системное событие состоит в завершении текущего задания, то специфические действия заключаются в возможной корректировке значения времени отклика соответствующей задачи:

```
int job_resp = cur_time -
    EventList.Next->Job_ptr->Start_time;
if(ReadyList.Next->Task_ptr->Period < job_resp)
    ReadyList.Next->Task_ptr->Period = job_resp;
```

Значение context_switchs увеличивается на единицу.

Обязательные действия шага моделирования. После завершения специфических действий выполняются следующие обязательные для каждого шага моделирования операции.

а) Вычисляется предполагаемая длина очередного шага процесса моделирования

```
int step_length = EventList.Next->Ordering - cur_time;
```

б) Если список активных заданий `ReadyList` не пуст (`ReadyList.Next` не равен `NULL`) и значение атрибута `Rest_C_size` не превосходит `step_length`, то значение переменной `step_length` уменьшается до величины `Rest_C_size` текущего задания

```
step_length = ReadyList.Next->Rest_C_size;
```

В список системных событий вставляются новый элемент — дескриптор системного события, состоящего в завершении текущего задания со следующими значениями атрибутов:

```
Ordering = cur_time + step_length;
Event_type = 1;
Job_ptr = ReadyList.Next;
```

в) Для текущего задания уменьшается значение `Rest_C_size` не израсходованного заданием объема процессорного времени:

```
ReadyList.Next->Rest_C_size -= step_length;
```

г) Модифицируется значение текущего момента модельного времени:

```
cur_time = EventList.Next->Ordering;
```

д) Головной дескриптор списка системных событий удаляется из `EventList`:

```
EventList.Pop();
```

Головным в списке системных событий `EventList` становится дескриптор, следующий за удаленным дескриптором.

е) Проверяются условия завершения сеанса моделирования. Сеанс моделирования завершается либо в случае превышении счетчиком `cur_time` предельно допустимого значения (аномальная ситуация), либо в случае отсутствия активных заданий (то есть, если список `ReadyList` оказывается пустым – нормальное завершение сеанса).

Если условия завершения сеанса моделирования не выполнены, то по завершении перечисленных обязательных действий выполняется переход к следующему шагу моделирования.

5. Выход из сеанса моделирования. К моменту нормального выхода из сеанса моделирования атрибут `R_time` каждого объекта типа `Task` содержит значение времени отклика соответствующей задачи. Глобальная переменная `context_switchs` содержит число переключений контекста в рамках интервала модельного времени длиной `cur_time`.

Заключение. Образовательная система в информационном обществе должна стать системой опережающей. Переход от консервативной образовательной системы к опережающей должен базироваться на опережающем формировании информационного пространства Российского образования.

СПИСОК ЛИТЕРАТУРЫ

1. Давиденко К.Я. Технология программирования АСУТП. Проектирование систем реального времени, параллельных и распределенных приложений – М.: Энергоатомиздат, 1985, 183 с.
2. Liu J.W.S. Real-Time Systems – NJ: Prentice Hall, 2000, 380 p.
3. Laplante P.A. Real-Time Systems Design and Analysis – John Wiley & Sons, Inc., 2004. – 530 p.

УДК 004.78

ВЫЧИСЛИТЕЛЬНЫЙ ФОРМАЛИЗМ СИНТАКСИЧЕСКИ ВАРИАНТНОЙ СИСТЕМЫ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО МОНИТОРИНГА ГЕТЕРОГЕННЫХ СЕТЕЙ СВЯЗИ

Олимпиев Алексей Александрович,
ЗАО «Институт инфотелекоммуникаций»,
Россия, Санкт-Петербург, Кантемировская ул., д. 5,
e-mail: oaa_82@mail.ru

Аннотация: В статье описана логическая структура системы оперативно-технического мониторинга с метауправлением, рассмотрены основные механизмы, реализующие синтаксическую вариантность ее компонентов, представлен язык реализации функциональности и особенности языка описания функциональности.

Ключевые слова: сетевой мониторинг, метауправление, метаинформация, объектная модель.

COMPUTATION FORMALISM OF VARIABLE SYNTAX MONITORING SYSTEM WITH SYNTATIC VARIANCE

Olimpiev Alexey,
JSC "Institute infotelecommunications"
Russia, St. Petersburg, Kantemirovskaya ul., D. 5,
e-mail: oaa_82@mail.ru

Abstract: The article describes the logical structure of the network monitoring system with functionality metacontrol, the basic mechanisms that implement syntactic variance components, the language of functionality implementation and features of the language of specification the functionality.

Keywords: *network monitoring, metacontrol, metainformation, object model.*

Введение. Система оперативно-технического мониторинга (СОТМ) сетей связи является подсистемой автоматизированной системы управления связью (АСУС). Ее свойства определяют возможности АСУС в части сбора, хранения, обработки и предоставления данных оперативно-технического мониторинга пользователю – информационной поддержке принятия решений. Особую роль СОТМ играет в сетях связи специального назначения (СССН), являющихся гетерогенными не только с точки зрения структуры и содержания, но и с точки зрения многообразия используемых интерфейсов и протоколов управления.

К СОТМ в СССН предъявляются жесткие требования, к которым, в частности, относятся:

– требование к полноте охвата СССН как объекта мониторинга и возможности гибкой настройки критериев оценки качества функционирования сетевых элементов и СССН в целом;

– требование к адаптируемости – СОТМ должна приспосабливаться к изменениям условий функционирования (эволюционным и/или оперативным изменением обстановки) в части учета этих изменений в информационной модели СССН и в правилах оценки качества функционирования;

– требование к оперативности и непрерывности сбора данных мониторинга и унифицированного отображения этих данных в информационной модели СССН;

– специальные требования, предъявляемые к прикладному программному обеспечению (ППО), применяемому в СССН – проведение сертификационных испытаний и фиксация состояния (контрольных сумм) СОТМ как изделия, любые изменения которого требует повторной сертификации.

Предъявляемые требования препятствуют выбору готового решения, доступного на рынке, для создания СОТМ в СССН, так как содержат очевидные противоречия:

– противоречие между свойствами мониторируемых СССН (динамичность и гетерогенность номенклатуры мониторируемых объектов, эволюционный характер развития) и необходимостью в полноте охвата их элементов в ППО СОТМ, где в основном используются фиксированные информационные модели и алгоритмы;

– противоречие между необходимостью внесения изменений в ППО СОТМ, связанных с первым противоречием, и необходимостью фиксации состояния (контрольных сумм) ППО, используемого в СССН, до начала его эксплуатации, что чревато внесением программных ошибок и приводит к необходимости повторного развертывания СОТМ в СССН (перерывах в функционировании).

Анализ предлагаемых на рынке адаптируемых СОТМ показывает, что существующие методы адаптации сводится к наращиванию ППО разного рода программными модулями, каждый из которых также требует сертификации, денежных затрат и привлечения команд разработчиков.

Методы разрешения описанной проблемы следует искать в методологии метауправления функциональностью (МУФ) информационных систем (ИС) [1], которая позволяет создавать ППО, адаптируемое в тех или иных ограниченных пределах к изменению условий применения посредством импорта компонентов метаинформации и последующей интерпретацией их вычислительной и прикладной семантики в рамках вычислительного формализма синтаксически вариантных ИС. Применение МУФ во много раз снижает вероятность возникновения условий, требующих внесения изменений в программный код СОТМ и, следовательно, не требуют проведения повторной сертификации – адаптация происходит без перерывов в работе СОТМ и дополнительных финансовых затрат и может выполняться службой эксплуатации (при условии достаточной квалификации персонала).

Для формализации вычислительного процесса, сопровождающего решение задачи оперативно-технического мониторинга, проведен анализ рекомендуемой для использования в СССН физической структуры СОТМ с учетом предположения о применении в ней методов МУФ. Это позволило выделить ключевые функциональные и информационные элементы [2] системы (см. рисунок 1):

– объектная модель (ОМ) СССН (ВИМ), представляющая собой базу данных фиксированной структуры, содержащую актуальное состояние ОМ в виде абстракций «объект», «объект-атрибут» и «объект-связь-объект» без учета принадлежности объектов множеству классов;

– диспетчер объектов (ДО, АУИМ), который выполняет функции по ведению ОМ СССН (ВИМ) в части создания/удаления объектов и связей, а также являющийся транспортом для передачи объектам сообщений, поступающих от медиаторов (А(i)МЕД, i = [1..N], N – мн-во контрольных точек технологического мониторинга (ТМ)), пользователей (ХПОЛЬЗ), самого ДО и отдельных объектов на этапе их функционирования;

– множество медиаторов (А(i)МЕД), размещенных в контрольных точках ТМ, предназначенных для взаимодействия со средствами технологического управления (Х(i)ТУ, каждой контрольной точке ТМ поставлен в соответствие медиатор) и выполняющих действия по преобразованию абстракций ТМ к значениям атрибутов ОМ;

– семантическая сеть «класс сетевого элемента» (ВКМИ), представляющая собой базу данных фиксированной структуры, содержащую коллекцию абстракций «класс сетевого элемента», связанных отношением наследования. Абстракция «семантическая сеть» включает в себя описание атрибутов и поведения объектов, а также правила преобразования данных ТМ функционально подобных средств телекоммуникации, являющихся объектами мониторинга уровня технологического управления, что позволяет отобразить особенности их функционирования на однородном множестве атрибутов объекта, т.е. в унифицированном виде;

– компилятор (АУКМИ) компонентов метаинформации (КМИ), выполняющий функции по управлению вычислительной и описательной способностью СОТМ за счет ведения иерархии классов (ВКМИ), управления алгоритмами функционирования ОМ и правилами преобразования данных ТМ к значениям атрибутов отдельных объектов;

– средства доступа к ОМ (АУВИМ) и управления ее содержанием (АУУС), предназначенные для взаимодействия СОТМ с пользователем (ХПОЛЬЗ) с целью предоставления ему актуальных сведений о состоянии объектов мониторинга, а также возможностей по управлению содержанием ОМ – занесение, корректировка и удаление учетных сведений (приведение информационной модели СССН в соответствие плану связи).

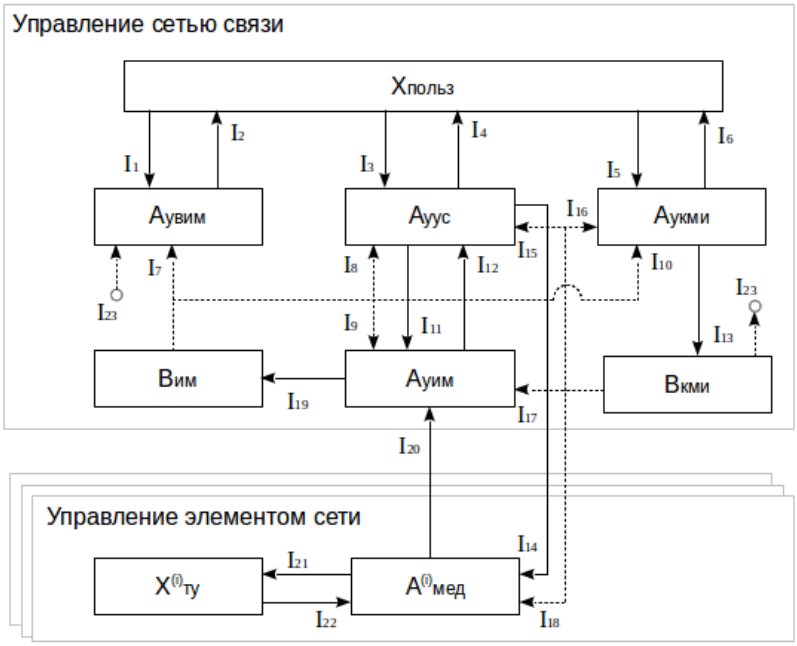


Рис. 1. Логическая структура СОТМ СССН

Множество информационно-управляющих каналов, связывающих функциональные элементы СОТМ $I = \{I_1 ... I_{23}\}$ может быть условно разделено на две группы:

– канал управления, образованный потоком управляющих воздействий, каждое из которых инициирует работу функционального элемента нижнего уровня (относительно инициатора воздействия), либо потоком выработанных реакций на предшествующее управляющее воздействие [3] (каналы управления на рисунке 1 показаны непрерывными линиями);

– «знание о» — вид информационного канала, по которому функциональному блоку доступна информация из блока информационного (канал информационного обеспечения подсистемы), этот вид взаимодействия на рисунке 1 показан пунктиром.

Разделение СОТМ СССН на функциональные и информационные элементы необходимо для самостоятельного рассмотрения процессов актуализации состояния ОМ, процессов управления вычислительной способностью (адаптации) и процессов взаимодействия с пользователем, что требуется [1] для исследования процессов МУФ синтаксически вариантной СОТМ.

Применение методологии МУФ позволяет рассматривать работу ДО, множества медиаторов и средств доступа к ОМ в контексте фиксированной вычислительной способности СОТМ, так как каждый из них не зависит непосредственно от актуального множества классов ($В_{КМИ}$), а процессы управления вычислительной способностью сделать зависимыми от текущего содержания ОМ ($В_{ИМ}$), что требуется для обеспечения целостности хранимых данных.

Рассмотрение совместной работы компилятора КМИ и ДО в контексте актуальной семантической сети «класс сетевого элемента», позволяет представить процессы формирования семантической сети и ОМ СССН как последовательность чередующихся этапов управления семантической сетью и ведения ОМ. В их совместной работе заключается вычислительный процесс

«познавания» объекта мониторинга в СОТМ, являющийся ключевым процессом, заложенным в ее алгоритмический инвариант.

В то же время ОМ СССН, разработанная с использованием базовых положений объектно-ориентированного подхода к моделированию [3], в СОТМ имеет свои особенности:

– любому элементу сети поставлен в соответствие единственный объект модели;

– над объектами существует типовой набор связей, позволяющий описать существующие в действительности взаимодействия или отношения (мн-во троек объект-связь-объект определяют актуальную структуру ОМ в любой момент времени);

– подмножества объектов образуют классы, соответствующие функционально, логически, структурно или иначе подобным элементам сети;

– каждому объекту доступен набор методов класса, причем каждый метод содержит описание реакции этого объекта на возмущение окружающей среды – объектов, с которыми он связан, либо на изменение значений параметров функционирования его прототипа (поступление данных мониторинга средства телекоммуникаций);

– каждый объект может быть представлен как абстрактный автомат, такты работы которого приводят к вычислению его состояния, в котором учитываются не только значения собственных атрибутов объекта, но и доступные ему значения атрибутов соседей;

– в процессе работы объект формирует сообщения другим объектам об изменениях в значениях его атрибутов (каждый такт работы может быть сформировано более одного сообщения).

При повседневной эксплуатации СОТМ, работа ОМ инициируется медиаторами, которые используют коллекцию правил преобразования данных ТМ. Актуализация этих правил происходит централизованно для всех медиаторов [4], где есть элементы соответствующего класса, что совместно с формированием семантической сети рассматривается как процесс управления вычислительной способностью (процесс адаптации). Если управление вычислительной способностью СОТМ рассматривается как увеличение глубины охвата сети (степени детализации обозреваемых средств телекоммуникаций и их характеристик), то управление охватом СССН вширь осуществляется пользователем, который вводит учетные сведения, изменяет правила и критерии оценки состояния элементов сети, которые сохраняются в атрибутах объектов и учитываются при вычислениях.

Для реализации работы средств визуализации ОМ СССН ($A_{УВИМ}$) используется утверждение о том, что структура каждого объекта не зависит от класса, которому он принадлежит, на содержание экранной формы влияют только атрибуты объекта, построенные посредством агрегации базовых типов, что позволяет формализовать процесс визуализации ОМ, как описано в [5] и создать условия для применения шаблонного подхода к описанию экранных форм. В свою очередь работа средств управления содержанием ОМ СССН (средства ввода информации, $A_{УУС}$) полностью зависит от содержания ($B_{КМИ}$), так как должна быть направлена на поддержку непротиворечивости вводимой информации и корректировку действий пользователя.

Каждое действие, направленное на изменение состояния или содержание ОМ производится через ДО, что делает его центральным элементом синтаксически вариантной СОТМ СССН. ДО представляет собой суперпозицию управляющих алгоритмов ведения ОМ и имеет фиксированную на этапе реализации структуру (см. рисунок 2), что означает отсутствие в ней каких-либо зависимостей от классов сетевых элементов и содержимого ОМ. Особенности ОМ, описанные выше, являются ключом к формализации вычислительного процесса, протекающего в ДО и позволяющего представить его в виде виртуальной машины [6]. Управление виртуальной машиной производится с помощью предложений на языке сценариев синтеза ОМ (ЯСОМ), который является разновидностью языка реализации функциональности ИС [1]. ЯСОМ можно описать следующей грамматикой:

SS := T1|T2|T3|T4|T5|ε

T1 := <создать объект, класс, имя, параметры>

T2 := <удалить объект, имя>

T3 := <связать объекты, имя1, имя2, тип связи, параметры>

T4 := <удалить связь, имя1, имя2, тип связи>

T5 := <передать сообщение объекту, сообщение, имя, параметры>.

Как и положено любому языку реализации функциональности смысл предложений на ЯСОМ зависит от содержания семантической сети, синтаксис которой в свою очередь описывается с помощью языка описания функциональности — декларативного предметно-ориентированного языка, который в данном случае включает абстракции вычислений (описания алгоритмов), требующиеся для реализации правил преобразования данных технологического мониторинга и правил обработки сообщений (методов классов объектов).

Предложения ЯСОМ, обозначенные на рисунке 2 буквой X, могут поступать от разных источников (средства управления содержанием ОМ, медиатор, ДО и объекты) и представляют собой инструкции, которые ДО должен выполнить для перевода ОМ в целевое состояние. Обработка инструкций происходит строго последовательно для обеспечения целостности ОМи СССН. В результате каждого такта работы, ДО выполняет одно из следующих действий: создает объект, производит удаление объекта, создает или разрывает связь между объектами, либо изменяет

значения атрибутов объектов. Для выполнения каждого из эти действий ДО обращается по каналу I_{17} (см. рисунок 1) за информацией, содержащей правила интерпретации инструкции, а также описания методов объектов. О завершении действия ДО информирует объект, на который это действие было направлено (отправляет ему сообщение). Так как правила вычисления состояния объектов могут меняться «налету» за счет описанного ранее механизма управления вычислительной способностью, в ДО дополнительно предусмотрен «триггер» обнуления состояния объектов, принадлежащих изменившемуся классу.

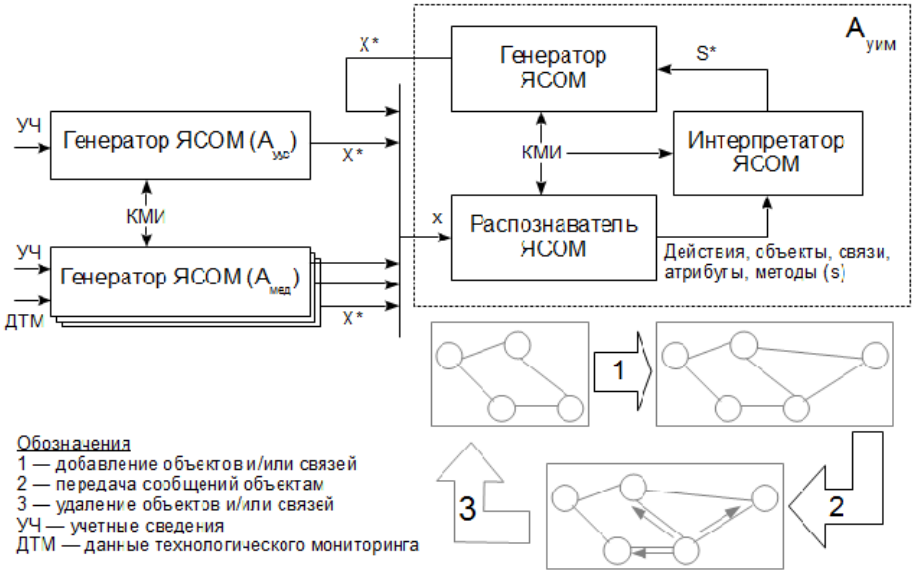


Рис. 2. Алгоритмическая модель диспетчера объектов

Интерпретация любого предложения ЯСОМ включает три базовых этапа: распознавание и интерпретация предложения, на которое указывает курсор ДО, и генерация нового предложения, содержащего сведения о произошедших в ОМ изменениях. Распознавание инструкции позволяет определить целевой объект (объекты), а ее интерпретация заключается в передаче управления методу объекта, инициируя его работу как автомата посредством отправки ему сообщения (S). Результат обработки сообщения используется для генерации нового предложения ЯСОМ, которое помещается в начало входной очереди.

При реализации ДО должен быть учтен тот факт, что инструкции, сформированные им самим всегда протекают в рамках одной транзакции, которая начата по инициативе внешнего источника, — возникновение ошибки времени выполнения должно приводить к откату всей текущей транзакции. Ошибки времени выполнения являются ожидаемыми и могут возникать (при условии безошибочной работы ДО) при выполнении метода объекта (вероятностью написания алгоритма вычисления оценки состояния объекта или преобразования данных технологического мониторинга с ошибкой не следует пренебрегать). Возникновение таких ошибок должно максимально полно исключаться на этапе компиляции КМИ [4], так как подобного рода ошибки могут привести к невосполнимым потерям существенной информации.

Требование полного исключения компилятором ошибок приводит к известному [6] противоречию, связанному с разработкой языка описания функциональности – простота языка противопоставляется его выразительности, что следует учитывать при его формализации.

Если для реализации декларативной составляющей языка описания функциональности может быть, например, использован один из множества существующих диалектов специфицирования на платформе XML, то средства описания алгоритмов следует рассмотреть отдельно. Из изложенного выше следует, что эти средства должны позволять описывать следующие действия:

– преобразование примитивных типов данных, которое будут встречаться при отображении данных технологического мониторинга к значениям атрибутов объектов;

– обработка абстрактных типов данных, связанная с определением всех необходимых операторов [7], а также наиболее часто встречающихся алгоритмов (поиска, сортировки и др.) [8].

Учитывая место выполнения подпрограммы (ДО), полученной в результате компиляции описания метода объекта, следует отметить, что любые алгоритмы, приводящие к бесконечной последовательности действий, могут вывести ДО из строя (зациклить). Подобная ситуация усугубляет налагаемые на язык описания функциональности и компилятор ограничения, которые направлены на то, чтобы поставить императивную составляющую языка в полную зависимость от декларативной —

формализовать статическую семантику [6] языка описания функциональности и предопределить разнообразие возможных алгоритмов.

Анализ работы ДО, структуры ЯСОМ, особенностей ОМ, приведенных выше замечаний, базовых положений теории алгоритмов [8] и общих подходов к формализации абстрактных типов данных [7] позволяет сформулировать основные особенности языка описания функциональности, используемого в синтаксически вариантной СОТМ СССН, который должен включать:

– средства объявления классов объектов и типов связей между объектами;
– средства описания допустимых типов связей между объектами классов;
– средства импорта классов и описания правил наследования;
– базовые типы данных и базовые операции над ними;
– средства объединения базовых типов данных в абстракции более высокого порядка;
– средства объявления базовых типов для описания абстракций данных, используемых во взаимодействующих службах технологического управления, при этом объявления типов должно допускаться только в контексте описания правил преобразования, но не в методах объектов;
– средства описания абстракций алгоритмов (описания вычислений оценок состояний и правил преобразования данных технологического мониторинга), которые исключают возможность создания итераций с количеством повторов, превышающих фиксированное значение.

Язык не должен иметь средств взаимодействия с ресурсами вычислительной машины, при этом он должен базироваться на строгой типизации по именам [6]. Для любого нового класса должен быть предопределен фиксированный набор методов (полиморфизм объектной модели).

Опыт практической реализации описанной системы показал, что для описания поведения объектов достаточным является набор из следующих четырех методов (типов сообщений): объект создан, изменилось окружение, изменились параметры целеполагания, изменились параметры функционирования – этот вывод происходит из того факта, что другие интуитивно-ожидаемые методы объектов являются типовыми и не требуют своей реализации через метауправление.

Заключение. Описанный формализм может быть использован не только в СОТМ СССН, но и в системах мониторинга любого вида, где требуется применение МУФ. Отдельные части описанного формализма, с небольшими изменениями могут иметь иные направления применения, например, при реализации средств имитационного моделирования структурной динамики сложных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Шерстюк Ю. М. Основы метауправления функциональностью в информационных системах. – СПб.: СПИИРАН, 2000. – 155 с.
2. Гвардейцев М. И., Морозов В. П. Розенберг В. Я. Специальное математическое обеспечение управления, 2-е изд. – М.: Сов. радио, 1980. – 536 с.
3. Шлеер С., Меллор С. Объектно-ориентированный анализ: моделирование мира в состояниях. - Киев: Диалектика, 1993. – 240 с.
4. Зарипов В.Д. Олимпиев А.А., Шерстюк Ю.М., Рожнов М.Д. Модель регистрации и обновления компонентов метаинформации в распределенных системах мониторинга // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 90–94.
5. Олимпиев А. А., Шерстюк Ю. М. Отображение объектной модели сети связи в интерфейсе пользователя // Телекоммуникационные технологии. 2007. Вып. 3. с. 28–33.
6. Себеста Роберт У. Основные концепции языков программирования 5-е изд. – М.: Вильямс. 2001. – 672 с.
7. Альфред В. Ахо, Джон Хопкрофт, Джеффри Д. Ульман. Структуры данных и алгоритмы. – М.: Вильямс, 2003. – 383 с.
8. Кормен Томас Х., Лейзерсон Чарльз И., Ривест Рональд Л., Штайн Клиффорд. Алгоритмы: построение и анализ, 2-е издание. Пер. с англ. – М.: Издательский дом "Вильямс", 2005. – 1296 с.

УДК 681.3.06

МНОГОКРИТЕРИАЛЬНОЕ ПЛАНИРОВАНИЕ МОДЕРНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ УНАСЛЕДОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Вашко Вадим Юрьевич[3], Ковалев Александр Павлович[2], Семенков Олег Игнатьевич[3],
Зеленцов Вячеслав Алексеевич[1], Потрясаев Семен Алексеевич[1],
Соколов Борис Владимирович[1],
[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
[2] Федеральное государственное унитарное предприятие
«Конструкторское бюро «Арсенал» имени М.В. Фрунзе»
Россия, Санкт-Петербург, ул. Комсомола, 1–3
[3] Объединенный институт проблем информатики Национальной академии наук Беларуси»
Беларусь, 220012, Минск, ул. Сурганова, 6
e-mail: sokol@iias.spb.su, kbarsenal@peterlink.ru; vasko_vasko@mail.ru

Аннотация. В докладе предложена постановка многокритериальной задачи планирования модернизации и функционирования унаследованной информационной системы (УИС), которая свелась к задаче однокритериальной оптимизации на комплексе аналитико-имитационных моделей большой размерности. В результате проведенных исследований была разработана оригинальная

многоэтапная процедура комплексного планирования модернизации и функционирования УИС с учётом факторов неопределенности, базирующаяся на фундаментальных и прикладных результатах, полученных в междисциплинарной отрасли системных знаний.

Ключевые слова: *планирование модернизации и функционирования, комбинированная оптимизация*.

MULTICRITERIA PLANNING OF MODERNIZATION AND FUNCTIONING OF THE INHERITED INFORMATION SYSTEM

Vadim Vashko[3], Alexander Kovalev[2], Oleg Semenkov[3],
Vyacheslav Zelentsov[1], Semen Potryasaev[1], Boris Sokolov[1]
St.Petersburg institute for informatics and automation of the Russian academy of sciences,
Russia, St. Petersburg, 14 line, 39,
e-mail: sokol@iias.spb.su
[2] Federal state unitary enterprise “Design organization “Arsenal” named after M.V.Frunze”
Russia, St. Petersburg, Komsomols str., 1-3
e-mail: kbarsenal@peterlink.ru
[3] The State Scientific Institution «The United Institute of Informatics Problems of the National Academy of Sciences of Belarus»
Belarus, Minsk, Surganova str., 6,
e-mail: vasko_vasko@mail.ru

Abstract: The article presents a statement of a planning multicriteria problem of modernization and functioning of the inherited information system (IIS) which was reduced to a one-criteria optimization problem on a complex of analitiko-imitating models of big dimension. As a result of the conducted researches the original multi-stage procedure of comprehensive planning of modernization and functioning of IIS taking into account uncertainty factors which bases on fundamental and applied results, gained in the interdisciplinary branch of system knowledge was developed

Keywords: *planning of modernization and functioning, the combined optimization.*

Введение. В докладе в качестве основных объектов исследований рассматривается унаследованные информационные системы (УИС) [1], [2]. Под данными системами понимают информационные системы, для которых используется эволюционный путь развития, т.е., другими словами, переход от их «старой» архитектуры к «новой» архитектуре осуществляется в течение заданных промежутков времени и состоит в плановой замене отдельных подсистем и элементов функционирующей УИС в целях повышения ее производительности и снижения затрат на эксплуатацию. Данный этап жизненного цикла УИС называют этапом модернизации[1].

Традиционно для принятия решения на проведение модернизации УИС необходимо решить следующие задачи: синтез облика модернизируемой УИС (ищется ответ на вопрос – что и когда надо модернизировать); определение срока (момента времени), к которому надо завершить модернизацию; синтез технологии модернизации (ищется ответ на вопрос – в какой последовательности надо проводить модернизацию); синтез плана проведения модернизации.

Проведенный анализ показывает, что задача планирования и управления модернизацией УИС должна решаться совместно с задачей планирования и управления функционированием УИС в целях обеспечения устойчивой текущей деятельности соответствующей бизнес-системы (БС), в интересах которой создавалась УИС. При этом само планирование и управление должно осуществляться комплексно и затрагивать все основные элементы и подсистемы существующей и создаваемой УИС [1], [2[, [3].

Это означает, что в процессе выбора программ модернизации облика данной системы каждый раз требуется обоснованно определять, в каком месте и в какое время должна быть произведена замена того или иного элемента структуры (структур) существующей УИС на новый, перспективный элемент. Кроме того, требуется проводить оценивание того, как влияют изменения структур УИС на процесс функционирования БС, Для этого должна использоваться соответствующая система показателей эффективности и качества планирования модернизации (функционирования) УИС.

К числу таких показателей будем, в первую очередь, относить [4], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]: показатели эффективности применения УИС, которые включают в себя показатели её целевых возможностей и показатели устойчивости функционирования; показатели технической эффективности, к которым, в первую очередь, можно отнести пропускную способность, показатели оперативности реализации технологии управления УИС, эксплуатационные показатели (например, ремонтопригодность), эргономические и социально-психологические показатели; показатели экономической эффективности и ресурсосберегаемости (например, показатели полных затрат на модернизацию и функционирование УИС, время полной окупаемости системы, показатели расхода

(сбережения) ресурсов всех видов, полноты их использования на всех этапах ЖЦ УИС); показатели, характеризующие эффективность адаптации и самоорганизации УИС на этапе её модернизации и функционирования (показатели структурной и функциональной избыточности, показатели гибкости (адаптируемости) структур УИС, показатели сложности указанных структур); показатели, характеризующие длительность реализационного периода УИС (время проектирования модернизации УИС) и периода полезной жизни до следующей модернизации (время эксплуатации); показатели эффективности управления функционированием и модернизации УИС (в том числе показатели обоснованности принимаемых решений).

Проведенный анализ показал, что совместное решение задач комплексного планирования модернизации и функционирования УИС наряду с заданием перечисленных показателей предполагает: построение соответствующего полимодельного комплекса, описывающего все основные аспекты исследуемых процессов; разработку комбинированных методов, алгоритмов и методик многокритериального полимодельного синтеза программ управления модернизацией и функционированием существующей и внедряемой УИС.

Решение перечисленных задач многокритериального оценивания, анализа и выбора эффективных вариантов программ управления модернизацией и функционирования УИС в докладе предлагается осуществлять с использованием теории управления структурной динамикой (УСД) сложных объектов (СлО). Данная теория имеет междисциплинарный характер и основывается на результатах, полученных к настоящему времени в классической теории управления и исследовании операций, в общей теории систем и системном анализе, а также в искусственном интеллекте [2], [3], [8], [9], [10], [11], [12], [13], [14], [15].

Предлагаемый подход к решению проблемы планирования модернизации и функционирования унаследованной информационной системы. Главная особенность совместного решения задач планирования и управления модернизацией УИС, связана с существенной априорной неопределённостью исходной информации о состоянии рассматриваемой системы, особенно на ранних этапах принятия решений о ее модернизации. Так, рациональные требований к УИС на стадии внешнего проектирования приходится выбирать в условиях большой степени неопределённости, так как период использования модернизируемой системы по назначению отдалён по времени иногда на довольно большой срок; система предпочтений заказчика на стадии внешнего проектирования ещё недостаточно чётко выявлена; кроме того, слабо структурировано множество целей и задач, а множество допустимых стратегий (управлений) на каждом этапе жизненного цикла достаточно велико, а сами стратегии разнообразны. По мере реализации макроопераций, описывающих этапы жизненного цикла УИС, степень неопределённости рассматриваемых ситуаций несколько уменьшается из-за того, что часть ранее неопределённых факторов становится известной. Например, на завершающей фазе внешнего проектирования становится известным перечень требований к УИС, так как уже выбран вариант системы из множества допустимых вариантов.

Введём следующие обозначения: $J_{\text{об}}^{(i)}(\vec{\mathbf{u}}(i))$, $J_{\text{об}}^{*(i)}$ – соответственно обобщённый показатель эффективности УИС на *i*-м этапе жизненного цикла УИС и его экстремальное значение; $\vec{\boldsymbol{u}}(i) \in \Delta^{(i)}$ – соответственно вектор и множество допустимой стратегии управления УИС на *i*-м этапе жизненного цикла; $\vec{\xi} \in \Xi^{(i)}$ – соответственно вектор и множество неопределённых факторов (возмущающих воздействий) на *i*-м этапе жизненного цикла. Тогда по мере выполнения этапов жизненного цикла УИС мощности множеств $\Delta^{(i)}, \Xi^{(i)}$ сокращаются, так как часть управляющих возмущающих воздействий на каждом предыдущем (*i*-ом этапе) становится на следующем этапе определёнными факторами, формирующими условие для реализации нового этапа обобщённой операции. На рис.1 приведена схема реализации рассматриваемых обобщённых макроопераций, на которой показано постепенное сужение множества допустимых стратегий при переходе от одного этапа жизненного цикла к другому. В этом случае множество определённых факторов расширяется вследствие поступления информации о решениях, принимаемых на каждом этапе жизненного цикла системы [2], [3], [15].

После каждого этапа жизненного цикла постепенно сокращается и объём системы, реализующей обобщённую операцию (системы управления жизненным циклом УИС). Системы управления жизненным циклом УИС на каждом из этапов, которые мы обозначим символами $S^{(i)}$, *i* = 1, 2, 3, 4; на рисунке 1 изображены частично перекрывающимися прямоугольниками [3]. Высота таких прямоугольников условно показывает глубину проработки вопросов создания УИС на соответствующем этапе; а сторона основания прямоугольника – широту охвата вопросов. Огибающая кривая в нижней части рисунка 1 показывает, как увеличивается глубина проработки и сокращается широта охвата вопросов с течением времени. Проведенный анализ показал, что центральной проблемой при решении задач управления УИС на различных этапах ее жизненного цикла была и остается проблема многокритериального структурно-функционального синтеза облика указанной системы. К настоящему времени наиболее перспективными являются следующие подходы к

решению данной проблемы и соответствующего класса задач [2], [3], [4], [5], [6], [7], [12], [13], [14], [15], [16]:

Вариант I. Постановка и решение задачи однокритериальной оптимизации программ управления модернизацией и функционированием УИС на аналитической модели большой размерности как задачи выбора, осуществляемого путем формальной декомпозиции и проведения оптимизации на частных моделях по частным показателям эффективности (ПЭ) с использованием того или иного правила согласования, обеспечивающего сходимость процесса оптимизации к решению исходной задачи. В частности, к таким вариантам поиска программ управления модернизацией и функционированием УИС сводятся подходы, основанные на методах, предложенных Данцигом-Вульфом и Корнаи-Липтаком.

Вариант II. Постановка задачи однокритериальной оптимизации программ управления модернизацией и функционированием УИС на имитационной модели большой размерности как задачи выбора, осуществляемого путем неформальной декомпозиции задачи, построения совокупности аналитических моделей, отражающих различные стороны функционирования системы и имеющих приемлемую размерность, согласования аналитических моделей по принципу Парето и проведения имитационных экспериментов с паретовскими альтернативами с целью поиска точки, доставляющей экстремум исходному показателю эффективности системы.

Вариант III. Постановка задачи многокритериальной оптимизации программ управления модернизацией и функционированием УИС на комплексе моделей как задачи выбора с многими отношениями предпочтения, осуществляемого путем задания множества Парето с помощью основополагающей многокритериальной модели, сужения этого множества на основе машинного анализа его свойств и введения соответствующей информации в ходе интерактивной процедуры, выполняемой ЛПР, лицом, обосновывающим решения (ЛОР) с ЭВМ, а также на основе привлечения дополнительных математических моделей, обеспечивающих последующее уточнение и сужение множества Парето вплоть до принятия единственного решения. Паретовский принцип согласования при условии дополнения его положениями о сужении множества Парето создает наиболее благоприятные возможности для принятия всесторонне обоснованных решений, основывающихся на анализе поведения различных показателей эффективности внутри этого множества. При этом важное значение имеет правильная разработка стратегии сужения множества допустимых альтернатив с привлечением компетентных специалистов и различных классов моделей (математических, логико-алгебраических, логико-лингвистических моделей).

В целом общая постановка задач планирования модернизации и функционирования УИС в условиях неопределённости и многокритериальности, по сути, сводится, во-первых, к построению множества допустимых альтернатив (допустимых планов) и, во-вторых, к поиску такой конкретной альтернативы (альтернатив), при которой результирующая функция выбора принимает экстремальное значение. В конечном счёте, в рамках концепции субъектно-объектного моделирования, для решения задач планирования модернизации и функционирования УИС необходимо на основе практической реализации принципа внешнего дополнения привнести в исходную постановку задачи такую информацию, которая позволит «снять» как критериальную, так и модельную неопределённость и свести решаемую задачу с неопределённостью к её детерминированному эквиваленту.

Особенности модельно-алгоритмической реализации предлагаемого подхода. В докладе предложена обобщенная процедура адаптивного выбора и реализации программ управления УИС на различных этапах ее жизненного цикла, которая позволяет объединить все ранее полученные результаты в рассматриваемой предметной области. Данная процедура, базируется на комбинированном использовании результатов, полученных в рамках II и III подходов к решению задач многокритериального структурно-функционального синтеза, описанных в предыдущем пункте.

При разработке рассматриваемой обобщённой процедуры ее авторы исходили из наиболее общего сценария изменения внутренней и внешней обстановок, в рамках которых происходит функционирование и модернизация УИС. Пусть из-за воздействия возмущающих факторов (объективных, субъективных, внутренних, внешних), оказывающих влияние на УИС, находящейся на заданном этапе жизненного цикла в известном многоструктурном макросостоянии, возникает необходимость в решении следующих двух групп задач.

Во-первых, требуется найти новое многоструктурное макросостояние УИС, обеспечивающее эффективное её функционирование в складывающейся обстановке и, во-вторых, необходимо найти и реализовать такие программы управления структурной динамикой УИС, при которых обеспечивался бы как переход из заданного в синтезируемое многоструктурное макросостояние УИС, так и устойчивое управление функционированием УИС в промежуточных многоструктурных макросостояниях.

Предлагается следующий вариант решения перечисленных групп задач, включающий в себя две основные фазы [2], [10], [11]. На первой фазе должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний УИС или, говоря другими словами, структурно-функциональный синтез нового облика УИС, соответствующего складывающейся (прогнозируемой) обстановке.

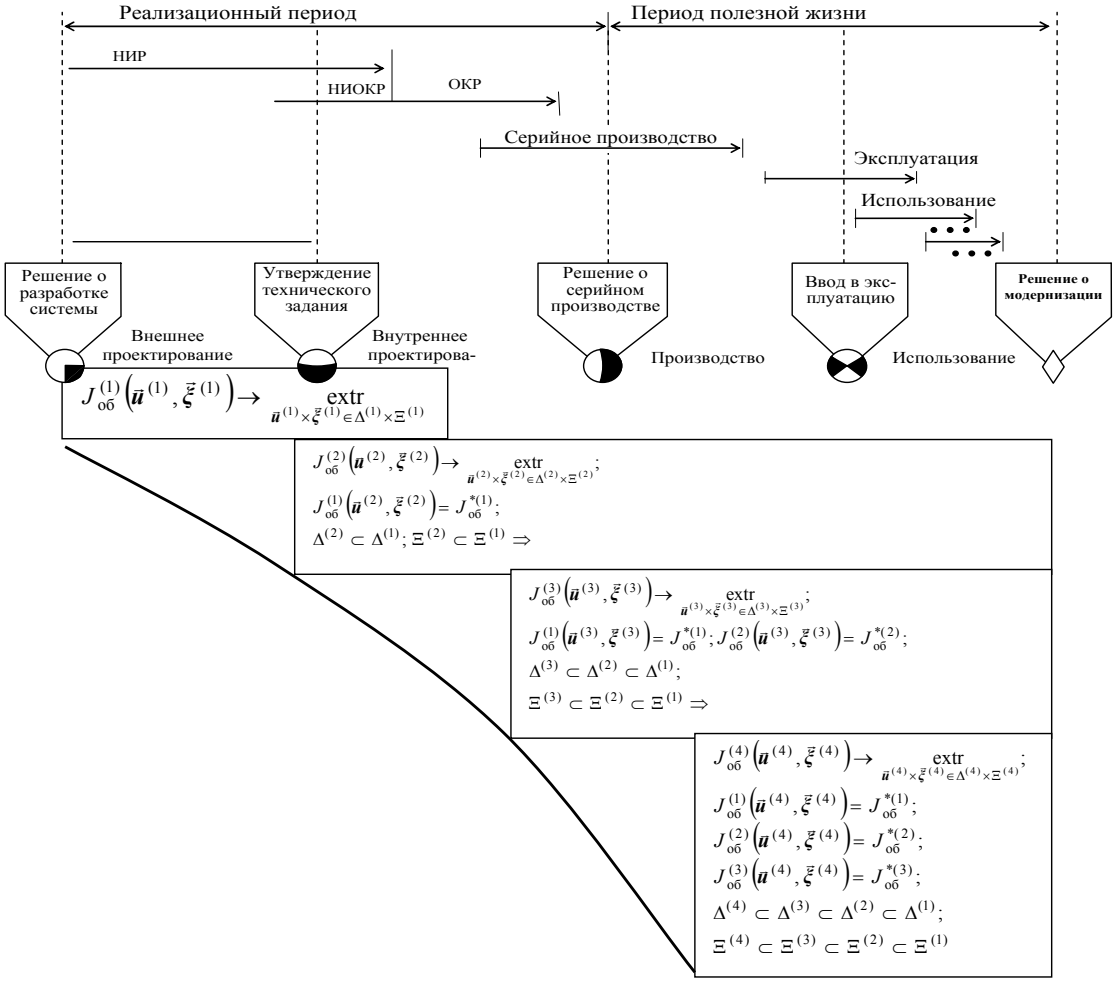


Рис. 1. Схема реализации обобщённых макроопераций на различных этапах жизненного цикла УИС

На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния УИС с одновременным синтезом (построением) адаптивных планов (программ) управления переходом УИС из текущего в требуемое (выбранное) макросостояние. При этом рассматриваемые планы должны обеспечивать такое эволюционное развитие УИС, при котором наряду с реализацией программ перехода из соответствующих макросостояний предусматривается одновременно и реализация программ устойчивого управления УИС в промежуточных многоструктурных макросостояниях.

На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния УИС с одновременным синтезом (построением) адаптивных планов (программ) управления переходом УИС из текущего в требуемое (выбранное) макросостояние. При этом рассматриваемые планы должны обеспечивать такое эволюционное развитие УИС, при котором наряду с реализацией программ перехода из соответствующих макросостояний предусматривается одновременно и реализация программ устойчивого управления УИС в промежуточных многоструктурных макросостояниях.

Проведенный в ходе выполненных исследований анализ показал, что много вариантность формального описания объектов управления и соответствующих управляющих подсистем, входящих в УИС, открывают широкие перспективы по постановке и решению задач адаптивного выбора (синтеза) комплекса моделей и алгоритмов программного управления и регулирования объектами в условиях постоянно изменяющейся обстановки. С учетом сказанного при модельно-алгоритмической реализации описанной процедуры было предложено ориентироваться на архитектуру современных имитационных систем (ИмС), в составе которой принято выделять [2], [3], [5], [6], [7], [15]: а) взаимосвязанный комплекс имитационных моделей (иерархии имитационных моделей), отражающих определённую проблемную область; б) взаимосвязанный комплекс аналитических моделей (иерархии аналитических моделей), дающих упрощённое (агрегированное) описание различных сторон моделируемых явлений; в) информационную подсистему, включающую базу (банк) данных, а в перспективе базу знаний, основанную на идеях искусственного интеллекта; г) распределенную систему управления и сопряжения, обеспечивающую взаимодействие всех компонент системы и работу с пользователем (лицом, принимающем решения) в режиме интерактивного диалога.

На аналитическом уровне описания процесс модернизации и функционирования УИС был интерпретирован как процесс выполнения комплексов целевых, обеспечивающих и вспомогательных операций, связанных с переходом УИС из одного многоструктурного макросостояния состояния в другое. При этом само многоструктурное состояние УИС характеризовалось заданной совокупностью параметров соответствующих операций, то есть, рассматривалась динамическая интерпретация процессов выполнения операций в УИС. Для формального описания указанной выше задачи планирования операций и распределения ресурсов в УИС использовалось несколько моделей, отражающих различные аспекты её функционирования: модель программного управления операциями; модель программного управления движением; модель программного управления ресурсами; модель управления потоками; модель программного управления вспомогательными операциями. На основе указанных частных динамических моделей была сформирована обобщённая динамическая модель процессов функционирования УИС:

$$M = \left\{ \begin{array}{l} \vec{u}(t) \left| \dot{\vec{x}} = \vec{f}(\vec{x},\vec{u},t); \right. \\ \vec{h}_0\left(\vec{x}(t_0)\right) \le \vec{O}; \vec{h}_1\left(\vec{x}(t_f)\right) \le \vec{O}; \\ \vec{q}^{(1)}(\vec{x},\vec{u}) = \vec{O}; \vec{q}^{(2)}(\vec{x},\vec{u}) \le \vec{O} \end{array} \right\} \quad (1)$$

где $\vec{x} = \left\| \vec{x}^{(o)\mathrm{T}} \vec{x}^{(\kappa)\mathrm{T}} \vec{x}^{(\pi)\mathrm{T}} \vec{x}^{(c)\mathrm{T}} \right\|^{\mathrm{T}}$; $\vec{u} = \left\| \vec{u}^{(o)\mathrm{T}} \vec{u}^{(\kappa)\mathrm{T}} \vec{u}^{(\pi)\mathrm{T}} \vec{u}^{(c)\mathrm{T}} \right\|^{\mathrm{T}}$ – обобщённые векторы состояния и управления УИС; $\vec{h}_0, \vec{h}_1$ – известные вектор-функции, с помощью которых задаются краевые условия для вектора $\vec{x}$ в моменты времени начала и окончания периода планирования – $t = t_0$ и $t = t_f$; $\vec{q}^{(1)}, \vec{q}^{(2)}$ – векторные функции, с помощью которых задают основные пространственно-временные, технические и технологические ограничения, накладываемые на процесс функционирования УИС.

В состав детерминированной динамической рассматриваемой модели планирования должна входить система показателей качества планирования, задаваемая следующим векторным показателем:

$$\vec{J} = \left\| \vec{J}^{(o)\mathrm{T}} \vec{J}^{(\kappa)\mathrm{T}} \vec{J}^{(\pi)\mathrm{T}} \right\|^{\mathrm{T}}, \quad (2)$$

компонентами которого являются векторы частных показателей качества планирования.

Компоненты обобщённых векторов состояния, управления и показателей качества относятся к записанным ранее моделям. Задача планирования модернизации и функционирования УИС может быть сформулирована как следующая задача программного управления динамической системой необходимо найти такое допустимое управление $\vec{u}(t), t \in \left(t_0, t_f\right]$, которое удовлетворяет требуемым ограничениям $\vec{q}^{(1)}(\vec{x},\vec{u}) = \vec{O}; \vec{q}^{(2)}(\vec{x},\vec{u}) \le \vec{O}$ и переводит динамическую систему $\dot{\vec{x}} = \vec{f}(\vec{x},\vec{u},t)$ из заданного начального состояния $\vec{h}_0$ в заданное конечное состояние $\vec{h}_1$. Если таких управляющих воздействий (планов) будет несколько, то среди них необходимо выбрать самое наилучшее, при котором компоненты вектора принимают экстремальные значения.

Разработанный комбинированный алгоритм комплексного планирования операций и распределения ресурсов в УИС, позволил исходную задачу планирования, имеющую по своей «природе» дискретно-непрерывный характер, преобразовать с помощью принципа максимума Л.С. Понтрягина и метода локальных сечений Болтянского В.Г. в двухточечную краевую задачу, и использовать для её решения метод последовательных приближений [2], [9], [10], [11].

На имитационном уровне описания процесс модернизации и функционирования УИС интерпретировался как дискретно-событийный динамический процесс, описываемый в терминах современной теории сетей массового обслуживания [16]. Для конструктивного взаимодействия аналитических и имитационных моделей был также разработан комбинированный алгоритм, основанный на совместном использовании моделей и методов локальной и глобальной оптимизации (метод основных осей Брента Р.П. и метод «пси-преобразований» Чиченадзе В.К. [17], [18]). При этом одно из достоинств предложенного комбинированного подхода заключается в том, что как при итеративном поиске параметров УИС с использованием стохастических моделей и методов глобальной оптимизации, так и при формировании собственно плана модернизации и функционирования УИС с учётом факторов неопределённости, обеспечивается монотонная сходимость итеративных процессов как за счёт интерактивной гибкой настройки программного обеспечения, реализующего разработанные методы на ПЭВМ, так и на основе использования заранее введённой параметрической и структурной избыточности в соответствующие численные алгоритмы оптимизации.

Заключение. В докладе рассмотрена формальная постановка соответствующей задачи программного управления модернизацией и функционированием УИС, которая свелась к задаче однокритериальной оптимизации (выбора) на комплексе аналитико-имитационных моделей большой размерности. В результате проведенных исследований была разработана оригинальная многоэтапная процедура комплексного планирования модернизации и функционирования УИС с учётом факторов неопределенности. Главное преимущество предлагаемого подхода по сравнению с существующими заключается в комплексном динамическом (контекстном) учёте при планировании модернизации и функционирования УИС как различных типов ограничений, накладываемых на указанный процесс на различных этапах ее жизненного цикла, так и возможных классов возмущающих воздействий, влияющих на устойчивость построенных планов. При этом само планирование осуществлялось на основе одновременного комбинированного использования детерминированных и стохастических моделей. Исследования, выполненные по данной тематике, проводились при финансовой поддержке ведущих университетов Российской Федерации: СПбГПУ, ИТМО (субсидия 074–U01), Программы НТС Союзного государства «Мониторинг СГ» (проект 1.4.1–1), грантов РНФ №№15-07-08391, 15-08-08459, 14–21–00135, 14-11-00748, РФФИ №№12-07-00302, 13-07-00279, 13-08-00702, 13-08-01250, 13-07-12120, 13-06-0087, Программы фундаментальных исследований ОНИТ РАН (проект №2.11), проекта ESTLATRUS 2.1/ELRI -184/2011/14, проекта ESTLATRUS/1.2./ELRI-121/2011/13 «Baltic ICT Platform».

СПИСОК ЛИТЕРАТУРЫ

1. Юсупов Р.М., Заболотский В.П. Научно-методические основы информатизации.– СПб.: Наука, 2000.
2. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с.
3. Надёжность и эффективность в технике: Справочник в 10-ти т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М.: Машиностроение, 1988, т.3. Эффективность технических систем /Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова.
4. Краснощёков П.С., Морозов В.В., Фёдоров В.В. Декомпозиция в задачах проектирования. Изв. АН СССР. Техн. Кибернетика, 1979, 2. С. 7–18.
5. Технология системного моделирования / Е.Ф. Аврамчук, А.А. Вавилов, С.В. Емельянов и др.; Под общ. ред. С.В. Емельянова и др. – М.: Машиностроение; Берлин: Техника, 1988.
6. Павловский Ю.А. Имитационные модели и системы. – М.: Фазис, 2000.
7. Имитационное моделирование производственных систем / А.А. Вавилов, Д.Х. Имаев, В.И. Плескунин и др. – М.: Машиностроение; Берлин: Ферлаг Техник, 1983.
8. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. – М.: Высшая школа, 1989.
9. Калинин В.Н., Резников Б.А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987
10. Соколов Б.В., Юсупов Р.М. Комплексное моделирование функционирования автоматизированной системы управления навигационными космическими аппаратами // Проблемы управления и информатики.–2002.–№5.
11. Калинин В.Н, Соколов Б.В. Многомодельный подход к описанию процессов управления космическими средствами //Теория и системы управления.–.1995.–№1.
12. Ларичев О.И. Теория и методы принятия решений. – М.: Логос, 2000.
13. Кини Р.Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. – М.: Радио и связь, 1981.
14. Нечёткие множества в моделях управления и искусственного интеллекта / Под ред. Д.А. Поспелова. – М.: Наука, 1986.
15. Скурихин В.И., Забродский В.А., Копейченко Ю.В. Адаптивные системы управления машиностроительным производством. – М.: Машиностроение, 1989.
16. Кокорин С.В., Рыжиков Ю.И. Оптимизация параметров сетей массового обслуживания на основе комбинированного использования аналитических и имитационных моделей // Журнал «Приборостроение», 2010. Т. 53, № 11.
17. Чичинадзе, В.К. Решение невыпуклых нелинейных задач оптимизации. Метод пси-преобразования. М.: Наука, 1983.
18. Brent, R. P. Algorithms for minimization without derivatives. USA, NJ: Prentice-Hall Inc., 1973, pp 195.

УДК 681.51

SYNGT: ПРИМЕНЕНИЕ АТРИБУТОВ

Федорченко Людмила Николаевна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия В.О., д. 39,
e-mail: lnf@iias.spb.su

Аннотация: В статье рассматривается подход к реализации контекстных условий при построении синтаксического анализатора языка с использованием инструментального средства SynGT (Syntax Graph Transformations).

Ключевые слова*: КСР грамматика, синтаксическая граф-схема, атрибуты, трансляции.*

SYNGT:IMPLEMENTATION OF ATTRIBUTES

Ludmila Fedorchenko
The St. Petersburg Institute for informatics and Automation,
Russia, St. Petersburg, 14-line V.O. 39,
e-mail: lnf@iias.spb.su

Abstract: This article describes an attribute approach to the problem of implementation of context conditions using parser tool SynGT(Syntax Graph Transformations).

Keywords: *CFR grammar, syntax graph-scheme, attributes, translations.*

Введение. Современные системы построения трансляторов для корректного отображения транслируемого языка во внутреннее машинное представление используют информацию о языке, определяя его синтаксис и статическую семантику в виде специальной грамматики, которая кроме основной своей функции порождения предложений языка позволяет задавать трансляции, необходимые разработчикам.

В теоретических работах под синтаксисом понимают множество правил грамматики, а все остальное в определении языка относят к семантике. В этом случае семантику делят на две части: те свойства языка, которые можно проверить в процессе трансляции (компиляции), называют статической семантикой, а остальные свойства языка – динамической семантикой.

В данной работе будем полагать, что грамматика, определяющая тексты языка, называется синтаксисом, некоторые правила, относящиеся к правильному использованию слов языка, называются статической семантикой, тогда как под динамической семантикой понимается то, как может быть установлено I/O отображение, создаваемое программой в процессе исполнения.

Полагаем, что программа состоит из слов. В этом случае терминальные символы КС-грамматики будут словами языка.

В сравнении с естественными языками большинство языков программирования отличаются тем, что некоторые слова не имеют заранее определенного значения, или их значение определено частично. Необходимые атрибуты таких слов фиксируются только в программе. Например, идентификатор может обозначать либо тип константы или тип переменной, либо метку или операцию. В языке BASIC буква, за которой следует открывающая скобка, может обозначать либо одномерный, либо двумерный массив и т.д. Поэтому большинство языков программирования имеет встроенные механизмы проверки синтактико-семантических свойств языка для всех допустимых слов в программе.

В реальных компиляторах все синтаксические проверки осуществляются, как правило, с помощью таблиц, где регистрируются текущие атрибуты проанализированных слов (конструкций языка) при анализе слева направо по тексту программы.

Существует много простых языков для калькуляторов, промышленного, бытового оборудования и т.д., которые не обладают такой порождающей мощностью, как, к примеру, программы в ALGOL 68, Ada, Fortran-77, и каждое слово в них имеет заранее определенное значение. В этих случаях язык не имеет статической семантики, и с помощью контекстно-свободного синтаксиса можно проверить, является ли программа на таком простом языке формально корректной или нет.

В теории формальных языков (как части Computer Science) к настоящему времени создано достаточно много абстрактных формализмов для определения языков программирования. Работа по созданию таких формализмов велась с 50-х годов прошлого столетия в 3-х направлениях:

– заменой формализма КС-грамматики на более мощную грамматику;

– встраиванием атрибутов и предикатов (проверок) в КС-грамматику;

– введением и пошаговой модификацией состояний преобразователя, построенного по исходной грамматике.

В первом направлении были сделаны несколько безуспешных попыток до того момента, как была придумана грамматика А. ван Вейнгаардена, которая использовалась в определении языка Algol 68 [11], [12], [13].

Во втором направлении важной работой стала статья Д. Кнута [7], в которой описана идея о том, что каждая синтаксическая конструкция имеет наследуемые и синтезированные атрибуты. Затем появилась аффиксная грамматика Костера [8], [9], [10], в которой идея с атрибутами Кнута была более развита, и которая стала теоретическим базисом для языка CDL [10], [14]. Функциональные грамматики тоже относится к этому направлению. Помимо Кнута похожий метод был предложен Гриффитсом (M.Griffits) [17].

Третье направление, которое основывается на работе Ледгарда (H.F.Ledgard) [15], было практически использовано в работах Вильямса (M.H.Williams) [16] и др. В этом случае имеется таблица (или что-то подобное ей), содержащая текущие имена с текущими атрибутами, и есть множество функций, которые связаны с синтаксическими конструкциями для модификации состояний таблицы. В таком методе терминальные символы КС-грамматики имеют функции перехода из состояния в состояние. Атрибуты для синтаксических единиц более высокого уровня вводятся так же, как в грамматике А. ван Вейнгаардена. Такой метод дал более ясное разделение между синтаксисом и статической семантикой.

1. Атрибутный подход. Понятие атрибута было введено Д. Кнутом [7] для описания семантики языков, порождаемых классическими контекстно-свободными грамматиками Хомского [1]. Атрибутный подход (по Кнуту) предполагает построение дерева разбора входного предложения языка в данной КС-грамматике, а затем вычисление значений атрибутов в каждой вершине этого дерева по правилам, связанным с правилами грамматики, участвующими в разборе. На практике данный подход был реализован в ряде инструментальных систем построения компиляторов, таких как, например, YACC [6], Eli [4], CUP[17].

Начиная с 70-х годов, для определения синтаксиса КС-языков применяется их регулярная форма, – КСР-грамматики, RBNF-грамматики [20], EBNF-грамматики и их графическое представление, – синтаксические граф-схемы (аналог диаграмм Н.Вирта [2]). Каждому нетерминалу соответствует одна компонента такой диаграммы или одно правило КСР-грамматики, правая часть которого является обобщённым регулярным выражением относительно символов объединенного алфавита грамматики [3], [19]. В объединённый алфавит грамматики входят алфавиты терминалов, нетерминалов, семантик и предикатов.

Технологии, использующие КС-грамматики с атрибутами (например, аффиксные грамматики), обычно преобразуют исходную грамматику в эквивалентную однозначную грамматику. В случае КСР-грамматики семантики и предикаты присутствуют в правилах наравне с терминальными символами, а в синтаксической граф-схеме (СГС) располагаются на дугах, соединяющих вершины, помеченные терминалами и нетерминалами.

За основу взята методика построения синтаксических таблиц состояний для языкового процессора, реализованная в инструментальной системе SynGT [3], использующая синтаксические граф-схемы и трансляционные КСР-грамматики для определения трансляций. Далее кратко опишем метод спецификации трансляций на трансляционных КСР-грамматиках и его использование при синтаксически-управляемой обработке данных в инструментальной системе.

2. Применяемая методика. Трансляция из языка $L_1 \subset \Sigma_1^*$ в язык $L_2 \subset \Sigma_2^*$ определяется как отношение $\tau \subset L_1 \times L_2$ [1]. На практике рассматривается обобщение этого определения, при котором трансляция определяет изменение состояния программы в зависимости от входного предложения.

В соответствии с требованиями [10], которым должно удовлетворять описание языка, способ спецификации трансляции должен давать следующее: возможность автоматического синтеза транслятора по спецификации; возможность анализа свойств входного языка; наглядность в описании синтаксиса и семантики входного языка.

Привлекательность КС-грамматик для анализа языка, их простота (правила имеют вид $A \to \alpha$, где α - цепочка символов из объединенного алфавита грамматики), позволяющая создавать эффективные анализаторы, породили огромное количество классов и подклассов грамматик, с различной степенью ограничений на языки. Наиболее сильные ограничения на языки (LL(k)), LR(k), LALR, SLR) позволяют строить анализаторы, имеющие линейную сложность разбора в зависимости от длины входного предложения.

Способ спецификации трансляций в системе SynGT позволяет определять контекстно-зависимые языки. Это достигается введением предикатов, ограничивающих выбор альтернатив при анализе входного предложения в зависимости от контекста. Состояние контекста изменяется семантиками, вводимыми непосредственно в текст грамматики или графа-схемы и обрабатываемыми наравне с терминальными символами. Предварительная обработка грамматики помимо выполнения различных эквивалентных преобразований транслирует предикаты и семантики в предикатные функции и семантические процедуры без параметров, создавая вычислительную надстройку. В этом случае атрибутные значения используются для параметризации семантических процедур и предикатных функций.

Следует отметить, что у Кнута семантика входного предложения определяется по его контекстно-свободной синтаксической структуре [7]. В случае *параметризации семантик* в SynGT атрибуты используются, как классические атрибуты Кнута. Но в методе Кнута правила вычисления атрибутов применяются после того, как дерево разбора входной цепочки в КС-грамматике уже построено. В системе SynGT семантика входного предложения определяется его контекстно-зависимой синтаксической структурой, что означает принципиальную невозможность отделить во времени процесс анализа от вычисления семантики.

При использовании атрибутов для *параметризации предикатов* принят метод параметризации нетерминалов аффиксами такой, как в системе CDL3 К. Костера[14]. Таким образом, атрибутная КСР-грамматика становится двухуровневой [10]. Известными представителями этого класса (двухуровневых) грамматик, помимо аффиксных грамматик К. Костера, являются также грамматики А. ван Вейнгаардена [13].

Как правило, используемые на практике искусственные языки, часто не являются контекстно-свободными. Применение двухуровневых грамматик, мощность которых достаточна для описания рекурсивных множеств, позволяет специфицировать синтаксис такого языка в рамках одного формализма и решить задачу обработки контекстных условий (статическая семантика).

В общем случае в SynGT используется синтаксический анализ типа top-down. Поэтому основным ограничением на класс грамматик является отсутствие леворекурсивных правил. Алгоритм преобразования грамматики с целью удаления любой рекурсии, в том числе и левой, в КСР-грамматиках подробно представлен в работах [18], [19]. Введение атрибутов в такой механизм анализа нуждается в разработке способа передачи контекстной информации только между процедурами анализа отдельных конструкций языка в процессе просмотра входного предложения. Процесс анализа

идет по нескольким параллельными маршрутами в синтаксической граф-схеме, представляющей КСР-грамматику. Для того, чтобы сохранить детерминированный характер этого процесса, на КСР-грамматику накладываются ограничения, которые учитываются при введении атрибутов.

Неформально можно провести аналогию используемого механизма анализа с анализом методом рекурсивного спуска в терминах множества конечных автоматов [3], взаимодействующих в общей операционной среде. Каждое правило КСР-грамматики, определяющее нетерминал A, отображается в описание процедуры A. Правая часть этого правила отображается в тело процедуры A, которое реализует проверку условий (бесконтекстных или контекстных), в зависимости от которых планируется соответствующая ветвь разбора. Бесконтекстное условие состоит в проверке того, что текущий входной символ равен соответствующему терминальному символу в правой части A-правила. Если это условие выполняется, то планируется продвижение по входному тексту и переход к следующей позиции в правой части A-правила. Если в текущей позиции правила для нетерминала A находится нетерминал B, то осуществляется вызов процедуры B, являющейся образом B-правила.

Контекстные условия реализуются соответствующими предикатными функциями, вызовы которых обозначены в рассматриваемом правиле семантиками или специфицированы на дугах в СГС. Вызовы семантических процедур в правой части правила также должны быть представлены явно.

Метод рекурсивного спуска в последовательной среде в общем случае сложен при реализации «отката» (back-tracking), то есть отмены семантических действий из-за нарушения бесконтекстных или контекстных условий на текущей ветви разбора. Поэтому применяемый в SynGT подход равносилен отображению нескольких правил в одну процедуру, что обеспечивает одновременное построение нескольких параллельных вариантов вывода с отбрасыванием недопустимых вариантов по ходу анализа. (см. определения состояния вершины в СГС и переходного состояния распознавателя).

Интерпретация метода рекурсивного спуска в терминах множества конечных автоматов [3], взаимодействующих в общей операционной среде, дает ключ к пониманию подхода к реализации атрибутов. Подобный подход успешно применялся в системе CDL с аффиксами и в последующих версиях CDL.

Продолжив аналогию с процедурами, можно каждому правилу сопоставить набор входных и выходных формальных параметров и локальных переменных. Элементы этого набора назовем формальными атрибутами. Для передачи информации в процедуры, соответствующие правилам грамматики или в процедуры, реализующие семантики и предикаты, можно применять наборы фактических параметров. Элементы таких наборов назовем фактическими атрибутами.

Таким образом, атрибуты на уровне грамматики описывают лишь порядок передачи контекстной информации между элементами конкретного алгоритма трансляции. Основной их задачей является доставка данных при реализации семантик и предикатов через параметры.

Поскольку возможные варианты продолжения анализа входной цепочки «тянутся» параллельно и фиксируются списками магазинов (см. определение состояния в СГС [3], [19]), то ограничения, накладываемые на КСР-грамматики в SynGT, допускают синтаксически неоднозначные грамматики при соблюдении локальной семантической однозначности с учетом детерминизма анализа. С другой стороны, исполнение семантических действий и, таким образом, изменение контекста и выполнение трансляции происходит одновременно с анализом входного предложения. Возможна ситуация, когда выполнение некоторого семантического действия зависит от информации, целиком доступной только к моменту окончания просмотра всего предложения языка. В этом случае такое действие может быть также отложено до стадии просмотра параллельных магазинов и вызова семантики в результате дополнительного анализа. На этом этапе происходит прохождение по состояниям анализатора в обратном порядке, вызов отложенных семантик и более точное определение синтаксической структуры входной цепочки с помощью предикатов.

При выполнении отложенных действий важно восстановить контекст, в котором эти действия были отложены. Иными словами, необходимо обеспечить передачу контекстной информации в таких особых случаях.

Неформальное определение атрибутной трансляции. Со всяким вхождением нетерминала в левые части правил связывается набор формальных атрибутов, а со всяким вхождением нетерминала, семантики или предиката в правые части правил набор фактических атрибутов. Формальные атрибуты делятся на наследуемые, синтезируемые и локальные атрибуты. Фактические атрибуты – на наследуемые и синтезируемые.

Предлагаемое определение атрибутной трансляции по своей сути близко к алгоритму Эрли [5], применяемому для анализа произвольных КС-грамматик. Метод рекурсивного спуска и преобразование правил грамматики в процедуры с параметрами аналогичен аффиксному подходу К. Костера. Основными отличиями являются учет контекстных условий, задаваемых предикатами, исполнение семантических действий, задание правил грамматики с помощью обобщённых регулярных выражений и применение атрибутов для передачи информации.

На основе алгоритма работы процессора и определения атрибутной трансляции выявляются и формулируются ограничения на атрибутную спецификацию трансляции, которые сводятся в основном к требованию отсутствия неопределённых значений.

Эти требование вытекает из общих ограничений на класс КСР-грамматик, применяемых в SynGT для получения детерминированных процессоров линейной сложности.

Атрибуты (как формальные, так и фактические) подразделяются на атрибуты прямого просмотра и отложенные, а некоторые локальные атрибуты могут определяться как двусторонние. Значения двусторонних атрибутов вычисляются на прямом просмотре и могут быть использованы в случае отложенности вычислений (когда просматриваются стеки в обратном порядке).

В ходе исполнения алгоритма трансляции процессор на отдельных участках входной цепочки ведет себя, как детерминированный конечный автомат (ДКА). В некоторых случаях работа такого ДКА приостанавливается, и управление передается другому автомату для анализа некоторой подконструкции. После окончания обработки подконструкции управление возвращается исходному автомату. Каждому такому ДКА соответствует одно или несколько правил грамматики. Значения формальных атрибутов, связанных с нетерминалами, входящими в левыех части правил, определяют локальный контекст автомата. Значения атрибутов считаются вычисленным к моменту достижения ДКА конечного состояния или исчерпанию входного текста. В этот момент эти значения должны быть записаны с тем, чтобы быть восстановленными в случае отложенных проверок. Запись происходит вместе с номером состояния, в которое осуществляется возврат управления, так называемого, возвратного состояния (второго элемента в списках пар состояний) (см. пример в [3]).

Передачи управления между конечными автоматами на отложенном просмотре согласованы и происходят при принятии возвратного состояния (второе состояние в паре (переходное, возвратное)). В этот момент формируется новый локальный контекст из значений отложенных атрибутов, значения двусторонних атрибутов восстанавливаются из соответствующей записи.

4. Модификация метода Кнута. При построении процессора языка его управляющая таблица дополняются таблицей контекстов, которые используется только на этапе синтеза процессора, и таблицей цепочек фактических атрибутов. Таблица контекстов связывает с каждым нетерминалом цепочку формальных атрибутов. Элементом такой цепочки является пара, состоящая из имени и класса атрибута. Таблица цепочек фактических атрибутов связывает с элементами правых частей правил наборы фактических атрибутов. Элементами такого набора являются следующие пары:

1) индекс формального атрибута, соответствующего нетерминалу, стоящему в левой части рассматриваемого правила; 2) класс фактического атрибута.

При проведении сравнения атрибутных подходов выявляются следующие основные преимущества атрибутных спецификаций в SynGT:

а) потоки данных задаются с использованием атрибутов независимо для каждого КСР-правила;

б) программисту-разработчику спецификаций для трансляции не приходится разрабатывать свой механизм передачи данных между семантиками и предикатами; такой механизм предоставляется самим алгоритмом трансляции;

в) обмен данных между семантиками и предикатами происходит через фактические параметры;

г) способ передачи информации в атрибутном подходе осуществляется через параметры процедур, связанных с синтаксической структурой входной цепочки.

Представленные в работе [3] ограничения на класс грамматик задают алгоритм проверки таких условий на уровне синтаксической граф-схемы.

Использование атрибутов во вспомогательных понятиях: вспомогательные понятия (новые нетерминалы, которые появляются в результате эквивалентных преобразований в SynGT и не являющиеся первоначальными грамматическими конструкциями), см. [3] в спецификациях на языке обобщённых регулярных выражений применяются для макроподстановок на этапе построения синтаксической граф-схемы. Использование атрибутов в спецификациях, таким образом, должно отразиться и на применении вспомогательных понятий. Эта проблема решается на этапе применения макроподстановки с помощью переименования атрибутов, так как в процессе регуляризации КСР-грамматики в результате подстановок «теряются» вхождения нетерминалов. **Контроль типов** значений атрибутов, может быть реализован на этапе построения управляющих таблиц. Кроме того, возможно осуществлять дополнительный контроль во время исполнения алгоритма трансляции, применяя предикаты. Описанный в [3] алгоритм оптимизации процессоров (минимизация числа состояний управляющей таблицы) основан на вычислении отношения эквивалентности для различных элементов управления процессора. Это отношение может быть модифицировано с учетом введения атрибутов. Сами алгоритмы оптимизации при этом не изменяются.

Заключение. Впервые атрибутная техника будет применяться непосредственно для регулярных выражений в правилах контекстно-свободной грамматики при построении языкового процессора в контексте следующих особенностей алгоритма трансляции: 1) атрибуты вычисляются в процессе построения дерева вывода, которое строится с учетом контекста, определяемого значениями атрибутов; 2) атрибуты применяются для контекстно-зависимого разрешения семантической неоднозначности трансляции. Полученные результаты развивают технологию синтаксически-

управляемой обработки данных с помощью инструментального комплекса SynGT, улучшая условия разработки и надежность информационных систем, создаваемых с ее использованием. Планируется реализация прототипа системы с атрибутами на платформе .NET. В качестве основы взят код инструментального комплекса SynGT, разработанного в СПИИРАН.

Использование разработанного прототипа предполагает следующее: 1) применение подхода с атрибутами улучшит условия разработки семантической части спецификации трансляции, избавляя разработчика от необходимости реализации своего метода передачи контекстной информации, согласованного с синтаксическим механизмом; 2) использование семантик и предикатов с параметрами сделает структуру семантической части спецификации более прозрачной и модульной.

СПИСОК ЛИТЕРАТУРЫ

1. Ахо А., Сети Р., Ульман Дж. Компиляторы: принципы, технологии и инструменты. Пер. с англ. М., 2001.
2. Вирт Н. Алгоритмы+структуры данных=программы. Пер. с англ. М., 1984 г.
3. Федорченко Л. Н. Книга – Регуляризация контекстно-свободных грамматик. Saarbrucken, Germany: LAP LAMBERT Academic Publishing GmbH & Co. KG Dudweiler Landstr. 99, 66123, 2011. 180 с.
4. Gray R.W., Heuring V.P., Levi S.P. et al. Eli: a complete, flexible compiler construction system // Communications of ACM, Vol. 35, Num. 2, 1992, pp. 121-130.
5. Early J. An Efficient Context-Free Parsing Algorithm // Communications of the ACM, Vol. 13, Num. 2, 1970, pp. 94-102.
6. Johnson S.C. Yacc yet another compiler compiler. Computer Science Technical Report 32. AT&T Bell Laboratories, Murray Hill, N.J., 1975.
7. Knuth D.E. Semantics of context-free languages // Mathematical Systems Theory 2:2. 1968, pp. 127-145.
8. Koster C.H.A. On the Construction of ALGOL-Procedures for Generating, Analyzing and Translating Sentences in Natural Languages. Report MR72, Mathematisch Centrum, Amsterdam, 1965.
9. Koster C.H.A. Affix Grammars // In: Proceedings of IFIP Conference on ALGOL 68 Implementation. 1970. Munich, pp. 95-109.
10. Koster C.H.A. Affix Grammars for Programming Languages // In: Attribute Grammars, Applications and Systems. International Summer School SAGA. 1991. Prague.
11. A. van Wijngaarden A. Orthogonal Design and Description of a Formal Language. Report MR76, Mathematisch Centrum, Amsterdam, 1965.
12. A. Van Wijngaarden et al.:"Report on the algorithmic language ALGOL 68" Numerische Mathematik 14, pp. 79–218 (1969) Springer-Verlag Berlin.
13. Revised report on the algorithmic language Algol 68"// ACTA Informatica 5 pp.1–236, (1974). In Russian "Пересмотренное сообщение о языке ALGOL 68".
14. Koster C.H.A., et all. CDL3 manual \\http://www.cs.ru.nl/ ~kees/vbcourse/ivbstuff/cdl3.pdf .
15. Ledgard H.F. "Production system or can we do better than BNF?" CACM 1974/2, pp.94–102.
16. Williams V.H. "Static semantics features of Algol 60, and BASIC". The Computer Journal. Vol. 21. No. 3. pp. 234–242.
17. Griffiths M. "Relationship between definition and implementation of language". //Advanced courses on software engineering. Lecture Notes in Economics and Math Syst. Springer-Verlag 1973.
18. Федорченко Л.Н, Извлечение крайней рекурсии из КСР-грамматики в системе SynGT, Труды СПИИРАН, вып.1,т. 1. — СПб: СПИИРАН, 2002, с.350–359.
19. Федорченко Л.Н. О регуляризации контекстно-свободных грамматик. // Изв. вузов. Приборостроение, 2006. Т.49, №11,с.50–54.
20. Лукичёв А.С. Использование атрибутов в технологии SYNTAX // Вест. Петерб. ун-та. Серия 1. Вып.2. СПб. 2005. С. 64-73

УДК 621.391.372

ОБ АДАПТИВНЫХ АЛГОРИТМАХ ППРЧ В УСЛОВИЯХ СЛУЧАЙНЫХ И ПРЕДНАМЕРЕННЫХ ПОМЕХ

Чуднов Александр Михайлович, Сапунова Лидия Петровна,
Военная академия связи имени Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., д. 3,
e-mails: chudnow@yandexl.ru, lidiya.karmanec@mail.ru

Аннотация: Рассмотрены принципы построения и оценки эффективности адаптивного алгоритма радиолинии с псевдослучайным переключением рабочих частот (ППРЧ), функционирующей в условиях случайных и преднамеренных помех. В теоретико-игровой постановке сформулированы оптимизационные задачи и приведен пример итеративной процедуры, обеспечивающей сходимость стратегий радиолинии и источника помехи к оптимальным. Приведены результаты расчетов, позволяющие оценить эффективность адаптивного алгоритма и скорость сходимости итеративных процедур.

Ключевые слова: *псевдослучайное переключение частот; расширение спектра; адаптивная радиолиния.*

ON ADAPTIVE ALGORITHMS FHSS UNDER RANDOM AND INTERNIONAL INTERFERENCE

Alexander Chudnov, Lidiya Sapunova,
The S. M. Budyonny Military Academy of Communications
Russia, St. Petersburg, Tihoretskii av., 3
e-mails: chudnow@yandexl.ru, lidiya.karmanec@mail.ru

Abstract: The article presents principles of construction and evaluation of an adaptive algorithm of pseudo-random frequency hopping spread spectrum (FHSS) radiolinks, functioning under a random and intentional interference. In the game-theoretic terms the problem of optimization is formulated and an example of an iterative procedure is given which ensures the convergence of strategies of the radiolink and the source of interference to the optimum. The results of calculations, allowing to evaluate the effectiveness of the adaptive algorithm and the convergence rate of iterative procedures, are given.

Keywords: *frequency hopping; spread spectrum; adaptive algorithm of radiolink.*

Введение. Одним из способов защиты радиолиний (РЛ) от преднамеренных помех является псевдослучайное переключение рабочих частот (ППРЧ) [1], [2], [3], [4], [5], [6]. Наиболее корректный анализ и синтез алгоритмов ППРЧ в условиях преднамеренных помех осуществляется методами теории игр, при этом в качестве противодействующих сторон принимаются система передачи информации (СПИ) и источник помехи (ИП). Исследования систем передачи информации методами теории игр проводились в работах [1], [2], [7], [8], [9], [10], [11], [12].

Хорошо изучены принципы построения теоретико-игровых алгоритмов переключения рабочих частот СПИ и стратегий постановки помех ИП в случае, когда условия прохождения сигналов от передатчика к приемнику на различных частотах одинаковы. При этом доказано (см. [1], [3]), что в достаточно общем случае оптимальный (равновесный в игровой задаче) алгоритм ППРЧ на каждом временном интервале выбирает для передачи информации рабочую частоту равновероятно из имеющейся совокупности частот, а оптимальная (равновесная) стратегия ИП распределяет равномерно среднюю мощность помех на совокупности рабочих частот радиолинии, причем «тонкая» структура помехи на каждой частоте оптимизируется с учетом характеристик РЛ и свойств среды распространения сигналов и помех. В частности, оптимальное подавление РЛ может быть реализовано путем равновероятного выбора с определенной периодичностью совокупности s (оптимальное число) подавляемых частот и воздействия на них с одинаковой мощностью.

В то же время при отсутствии преднамеренных помех, так называемый, адаптивный алгоритм управления радиолинией [13] состоит в определении наилучшей с позиции передачи информации частоты и использовании ее в качестве рабочей на анализируемом временном интервале. При изменении помеховой ситуации приемная сторона радиолинии посылает передатчику сигнал о необходимости перехода на другую (оптимальную) рабочую частоту.

В работе рассматривается радиолиния с адаптивным алгоритмом ППРЧ, предполагающим: 1) анализ приемной стороной помеховой ситуации в выделенном диапазоне частот; 2) определение оптимального для радиолинии распределения вероятностей на множестве допустимых частот; 3) определение соответствующего варианта (режима работы) ППРЧ, реализуемого с использованием криптографических средств; 4) передачу данных о варианте ППРЧ приемной стороной передатчику; 5) использование передатчиком и приемником радиолинии определенного в п. 3 варианта ППРЧ на заданном временном интервале. В отличие от работ [5], [6] решаемая задача направлена на отыскание оптимальных в игровом смысле (равновесных) алгоритма переключения частот радиолинией и алгоритма управления частотно-энергетическим ресурсом источника помехи. Для решения сформулированной игровой задачи используются итерационные процедуры [14], позволяющие осуществлять настройку алгоритмов РЛ и ИП в процессе функционирования СПИ.

Модель системы передачи информации (радиолинии) с ППРЧ и постановка задачи. Рассматривается радиолиния, в которой передача информации в каждый момент времени может осуществляться на одной из n выделенных частот. При этом передатчик и приемник радиолинии синхронно по неизвестному для источника преднамеренной помехи закону перестраиваются для работы на определенной частоте. В отличие от линий с простой программной ППРЧ изучается радиолиния, алгоритм выбора рабочей частоты которой может использовать информацию о состоянии совокупности выделенных частот с позиции возможности их использования для эффективной передачи информации.

При этом после вхождения в синхронизм и начала процесса передачи сообщений по заранее определенной процедуре ППРЧ (т.е. в заранее определенном режиме) работа радиолинии осуществляется следующим образом:

– на приемной стороне радиолинии в течение определенного времени проводится анализ состояния совокупности выделенных частот;

– по результатам анализа осуществляется расчет оптимальной (равновесной в теоретико-игровом смысле) совокупности параметров, определяющих целесообразный режим ППРЧ в данном состоянии среды распространения сигналов;

– данные о целесообразном режиме по обратному каналу передаются на передающую сторону радиолинии;

– в определенный момент времени передатчик и приемник переходят в новый режим ППРЧ.

С учетом конфликтности целей радиолинии и источника помехи, оптимизация и анализ осуществляются в рамках теоретико-игровой задачи. Используются следующие исходные данные: n

– число выделенных рабочих частот СПИ, $\delta_{\text{ср}}$ – отношение средней (приходящейся на одну рабочую частоту) мощности помехи к мощности сигнала, приведенное ко входу приемника радиолинии, $\varphi(i,\delta_{\text{i}})$ – функция (полагается непрерывной), характеризующая качество связи на i-й частоте при воздействии на этой частоте помехи с мощностью δ_{i}. В качестве такой функции удобно использовать зависимость вероятности ошибочного приема сигналов при различных способах формирования и приема сигналов с учетом свойств среды распространения сигналов на различных частотах. При этом для получения оценок эффективности адаптивного алгоритма ППРЧ в работе использовались зависимости, характеризующие вероятность ошибки при когерентном оптимальном приеме двоичных сигналов: $\varphi(i,\delta_{\text{i}}) = 1\text{-}\,F(h_i)$, где $F(h_i)$ – интеграл вероятностей Гаусса, $h_{\text{i}} = (\beta_i + \delta_i)^{-1/2}$, β_i – отношение мощности случайных помех (шумов) к мощности сигнала в точке приема. Символом P^n обозначается n-мерное евклидово пространство

Теоретико-игровая задача синтеза алгоритма управления радиолинией в условиях преднамеренных помех формулируется в терминах смешанных стратегий противодействующих сторон: радиолинии и источника помехи (см. [1], [3], [11], [12], [14], [15]). Смешанная стратегия радиолинии (алгоритм ППРЧ) задается распределением вероятностей $\mathbf{u} = (\mathrm{u}_1,...,\mathrm{u}_\mathrm{n})$, $\mathrm{u}_1 + ... + \mathrm{u}_\mathrm{n} = 1$ на множестве номеров частот, а смешанная стратегия источника помехи – функцией распределения вероятностей $V_{\boldsymbol{\delta}}(\boldsymbol{\delta})$ на множестве допустимых распределений помехи $\boldsymbol{\delta} = (\delta_1,...,\delta_n)$, определенном ограничениями на среднюю мощность источника помехи в виде:

$$\sum\nolimits_{i=1}^{n} \int_{\mathrm{P}^n} \delta_i dV_{\boldsymbol{\delta}}(\boldsymbol{\delta}) \le n\delta_{cp}\,. \tag{1}$$

Неравенство (1) можно и целесообразно преобразовать к более простому виду

$$\sum\nolimits_{i=1}^{n} \int_{-\infty}^{\infty} \delta_i dv_i(\delta_i) \le n\delta_{cp}\,, \tag{2}$$

где $v_i()$ – одномерная функция распределения вероятностей мощности помехи на i-й частоте, причем стратегия источника помехи может быть задана вектором $\mathbf{v} = (\mathrm{v}_1,...,\mathrm{v}_\mathrm{n})$, удовлетворяющим ограничениям (2).

Функция потерь РЛ (выигрыша источника помехи) в ситуации $(\mathbf{u},\mathbf{v})$, определенной выбором противодействующими сторонами стратегий $\mathbf{u},\mathbf{v}$, характеризуется вероятностью ошибочного приема сигналов приемником радиолинии, которая представляется выражением

$$p(\mathbf{u},\mathbf{v}) = \sum\nolimits_{i=1}^{n} u_i \int_{-\infty}^{\infty} \varphi\,(i,\delta_i)\, dv_i(\delta_i)\,. \tag{3}$$

Задачи синтеза алгоритма функционирования радиолинии с управляемым (адаптивным) ППРЧ в условиях оптимизированного подавления источником помехи состоит в определении допустимой стратегии $\mathbf{u}$, минимизирующей среднюю вероятность ошибочного приема сигналов (3) для наихудшей допустимой стратегии $\mathbf{v}$, и записывается в виде:

$$\sup\nolimits_{\mathbf{v}\in V}\, p(\mathbf{u},\mathbf{v}) \to \min\nolimits_{\mathbf{u}\in U}\,. \tag{4}$$

Аналогично двойственную задаче (4) задачу синтеза алгоритма функционирования ИП для РЛ с адаптивным ППРЧ можно представить соотношением

$$\inf\nolimits_{\mathbf{u}\in U}\, p(\mathbf{u},\mathbf{v}) \to \max\nolimits_{\mathbf{v}\in V}\,. \tag{5}$$

Пара двойственных минимаксной и максиминной задач (4), (5) составляют игру $\mathcal{G}(\mathcal{U},\mathcal{V},p())$, в которой множества допустимых стратегий игроков $\mathcal{U},\mathcal{V}$ (РЛ и ИП) определяются соотношениями:

$$\mathcal{U} = \{\mathbf{u} \in \mathrm{P}^n \,|\, \mathrm{u}_1 + ... + \mathrm{u}_\mathrm{n} = 1\},\ \ \mathcal{V} = \{\,\mathbf{v} \in \mathfrak{M}(\mathrm{P}^n) \,|\, \textit{выполняется}\,(2)\},$$

где $\mathfrak{M}(\mathrm{P}^n)$ – множество вероятностных мер на борелевской алгебре подмножеств P^n,
а функция **проигрыша** первого игрока определена выражением (3).

Важно отметить, что в силу компактности множества $\mathcal{U}$, слабой компактности множества $\mathcal{V}$ и непрерывности функции $p()$ в игре $\mathcal{G}(\mathcal{U},\mathcal{V},p())$ существует равновесная ситуация $(\mathbf{u}^*,\mathbf{v}^*)$. При этом: 1) в (4), (5) достигаются все минимумы и максимумы, 2) стратегии $\mathbf{u}^*,\mathbf{v}^*$ являются оптимальными как в прямой, так и двойственной оптимизационных задачах (4), (5), 3) изменение стратегии любой из сторон относительно оптимальной может привести лишь к понижению эффективности функционирования соответствующей системы в рассматриваемой задаче.

В [11], [16] рассмотрены примеры решения оптимизационных задач в моментных пространствах [17] (в том числе для оптимизации стратегии подавления РЛ с ППРЧ). Предложенная в указанных

работах методика основана на использовании теоремы Каратеодори [15], [17] и предполагает построение выпуклых оболочек оптимизируемых функционалов. Применительно к рассматриваемой задаче необходимо определить выпуклые сверху оболочки функций $\varphi(i,z)$ по аргументу z выражением:

$$\varphi^{\wedge}(i,z) = \max_{x,y,p:(1-p)x+py\le z}(1-p)\varphi(i,x)+p\varphi(i,y). \quad (6)$$

Как видно, в данном случае построение выпуклой оболочки функции сводится к задаче двухпараметрической оптимизации. При этом практически для всех используемых в приложениях функций $\varphi(i,z)$ оптимальная точка в (6) достигается при $x=0$, что сводит эту задачу к однопараметрической оптимизации. При выпуклости сверху функции $\varphi(i,z)$, очевидно, $\varphi^{\wedge}(i,z)=\varphi(i,z)$.

Использование функции $\varphi^{\wedge}(i,z)$ позволяет декомпозировать игру $\mathcal{G}(\mathcal{U},\mathcal{V},p())$ на внутреннюю оптимизационную задачу (6) и внешнюю игру $\mathcal{G}(\mathcal{U},\mathcal{W},p^{\wedge}())$, где $\mathcal{W}$ – множество допустимых стратегий ИП, определяемое соотношением $\mathcal{W}=\{\mathbf{w}\in \mathrm{P}^n \mid w_1+\ldots+w_n\le n\delta_{cp}\}$, а $p^{\wedge}()$ – функционал средней вероятности ошибки, представленный в виде:

$$p^{\wedge}(\mathbf{u},\mathbf{w}) = \sum_{i=1}^{n} u_i \varphi^{\wedge}(i,w_i). \quad (7)$$

Ситуация $(\mathbf{u},\mathbf{w})$ игры $\mathcal{G}(\mathcal{U},\mathcal{W},p^{\wedge}())$ имеет следующий физический смысл: РЛ, как и в игре $\mathcal{G}(\mathcal{U},\mathcal{V},p())$ использует для ППРЧ распределение вероятностей $\mathbf{u}=(u_1,...,u_n)$, ИП распределяет средние мощности помех в соответствии с вектором $\mathbf{u}=(u_1,...,u_n)$, а «тонкие» параметры стратегии ИП (вероятность выхода на определенную частоту в каждый момент времени и воздействующую при этом мощность) определяются на основе решения оптимизационной задачи (6).

Следует отметить, что, как правило, совокупность всех выделенных частот может быть разбита на относительно небольшое число групп эквивалентных по качеству прохождения сигналов частот. При этом все соотношения и постановка задачи остаются справедливыми, если участвующими в них величинами характеризовать не отдельные частоты, а группы в целом. В таком случае реализация источником помехи нужных значений параметров u_i может осуществляться путем постановки (с поэлементным перемешиванием) помех определенной мощности на подходящем числе частот.

Реализация итеративной процедуры и результаты расчетов. Для построения стратегий РЛ и ИП построен вариант итеративной процедуры поиска равновесных ситуаций [14] в виде последовательности вычислительных операций, предполагающих наличие у противодействующих сторон (поступление им) следующей информации:

– РЛ – о вероятностях ошибочного приема сигналов на каждой из частот. Эта информация может быть получена либо априорно от специального объекта, контролирующего состояние выделенных частот, либо апостериорно на основе статистики ошибок при прохождении информации на различных частотах.

– ИП – о частоте, на которой РЛ функционировала на предыдущем интервале времени.

Кроме того, полагалось, что инерционность контура подавления радиолинии источником помехи («прием сигналов РЛ – анализ ситуации – постановка помехи») достаточно велика, чтобы обеспечивалась невозможность подавления источником помехи текущей частоты передачи информации в РЛ (т. е. постановки помехи «вслед сигналу»).

В качестве функций $\varphi(i,\delta_i)$ использованы зависимости вероятности ошибки при когерентном оптимальном приеме двоичных сигналов в условиях гауссовского шума с неравномерной спектральной плотностью мощности в выделенном частотном диапазоне: $\varphi(i,\delta_i)=1\text{-}F(h_i),\ h_i=(\beta_i+\delta_i)^{-1/2}$. Предварительно задаются исходные данные: n – число частот, m – число групп эквивалентных частот, β_i – распределение случайных помех на выделенных частотах, δ_{cp} – средняя мощность ИП. $(\mathbf{u}(0),\mathbf{w}(0))$ – исходная ситуация, du – шаг перестройки вероятностей u_i, dw – шаг перестройки средних мощностей w_i и критерий останова процедуры.

Последовательность операций на каждом j-м, $j=1,2,...$, шаге процедуры следующая:

1. Вычисление вероятности ошибочного приема символов $p(\mathbf{u},\mathbf{w})$ на каждой из n выделенных частот.

2. Определение номера оптимальной рабочей частоты (группы частот) для использования РЛ на следующем шаге: $i(j)=\arg\min_i \varphi^{\wedge}(i,w_i)$.

3. Модификация стратегии РЛ: $u_{i(j)}(j) = u_{i(j)}(j-1) + du$, нормирование распределения вероятностей $\mathbf{u}$ с обеспечением $\mathbf{u} \in \mathcal{U}$.

4. Модификация стратегии ИП: $w_{i(j)}(j) = w_{i(j)}(j-1) + dw$, нормирование распределения мощностей $\mathbf{w}$ относительно $n\delta_{cp}$.

5. Проверка критерия останова, если не выполняется, то переход к п. 1.

В приведенном ниже примере расчетов полагалось, что случайные шумы в выделенном диапазоне имеют две составляющие: постоянную с относительной средней мощностью β_0 и переменную с относительной средней мощностью β_{cp}, распределенную по экспоненциальному закону $\beta_{1i} = \beta_{cp} k_0 \exp(k_1 i)$, где $k_0 = 1/\sum_{i=1}^{n} \exp(k_1 i)$ - нормирующий коэффициент, k_1 - показатель, характеризующий неравномерность распределения случайных помех в диапазоне частот, так что $\beta_i = \beta_0 + \beta_{1i}$.

В расчетах использовались следующие исходные данные: m=10, $\beta_0 = 0{,}05$, $\beta_{cp} = 0{,}1$, $k_1 = 3$, $du = dw = 0{,}1$. При этом расчеты осуществлялись для двух случаев: a) переход РЛ от работы на одной оптимальной частоте ($u_i = 1$) при появлении преднамеренной помехи к оптимальному распределению и b) переход РЛ от оптимального распределения к работе на одной частоте при выключении ИП. Полученные в результате расчетов значения величин, $p(\mathbf{u}, \mathbf{w})$ на различных шагах процесса приведены в таблице 1.

Таблица 1

Вероятность ошибочного приема двоичного символа в процессе настройки радиолинии при включении (процесс «a») и выключении (процесс «b») источника помехи.

n, δ_{cp}	Процесс	№ шага							
		0	4	8	12	16	20	24	∞
δ_{cp}=0,01 $n=10$	a	1,9E-02	1,0E-02	6,7E-03	5,0E-03	4,2E-03	4,2E-03	4,2E-03	4,2E-03
	b	4,5E-04	2,0E-04	9,7E-05	6,5E-05	6,2E-05	6,2E-05	6,2E-05	6,2E-05
δ_{cp}=0,01 $n=100$	a	1,7E-01	9,0E-02	4,9E-02	2,8E-02	1,9E-02	1,4E-02	1,2E-02	1,1E-02
	b	1,5E-04	1,2E-04	1,0E-04	8,5E-05	7,4E-05	6,7E-05	6,3E-05	6,2E-05
δ_{cp}=0,04 $n=10$	a	7,5E-02	4,1E-02	2,7E-02	2,0E-02	1,7E-02	1,6E-02	1,6E-02	1,6E-02
	b	1,5E-03	7,7E-04	2,7E-04	1,6E-04	1,6E-04	1,6E-04	1,6E-04	1,6E-04
δ_{cp}=0,04 $n=100$	a	3,1E-01	2,1E-01	1,4E-01	9,9E-02	7,3E-02	5,8E-02	5,0E-02	4,3E-02
	b	4,0E-04	3,2E-04	2,6E-04	2,2E-04	1,9E-04	1,7E-04	1,6E-04	1,6E-04

Как видно, в рассмотренных случаях процедура обеспечивает быструю сходимость стратегий РЛ и ИП к оптимальным. При увеличении числа рабочих частот сходимость процедуры ухудшается. Следует также отметить, что повышение точности описания случайных помех (в рамках определенного распределения их мощности по частотам) не приводит к заметному повышению точности решения рассматриваемых оптимизационных задач, но в то же время снижает скорость сходимости рассмотренной процедуры.

Заключение. Предложенный способ адаптивной перестройки алгоритма ППРЧ позволяет получить дополнительный выигрыш в эффективности функционирования радиолинии, который в зависимости от состояния случайных (взаимных) помех в выделенном диапазоне частот может составлять значительную величину. Итерационные процедуры поиска равновесных ситуаций, с одной стороны, обеспечивают возможность анализа эффективности подобных адаптивных алгоритмов и, с другой, могут непосредственно использоваться для управления режимами работы радиолинии в процессе ее функционирования. В последнем случае для управления радиолинией в реальном времени при наличии большого числа выделенных частот, по-видимому, потребуется оптимизация процедуры поиска равновесных ситуаций подходящими методами оптимизации в рамках теории игр [14], [15].

СПИСОК ЛИТЕРАТУРЫ

1. Жодзишский А.И., Жодзишский М.И. Потенциальные возможности командных радиолиний с дискретно изменяемой несущей частотой. РКТ, 1973, сер. VI, вып. 2 (11), С. 15-26.
2. Cook D.B. Interleavingm frequency hopping and spread spectrum for finite messages under jamming// Proc/ IEEE Nat/ Aerosp. and Electron. Conf.- NAECON'77.- Dayton, N.Y., 1977.- P.1300-1306. Kullstam P. A. Spread Spectrum Performance Analysis in Arbitrary Interference.— IEEE Trans. Commun, 1977, v. 25, №8. P. 848-853.
3. Чудное А. М. Помехозащищенность системы передачи информации с псевдослучайным переключением частот в условиях наихудших помех // Изв. вузов. Радиоэлектроника, 1984, т. 27, №9. С. 3—8.

4. Борисов В.И. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. - М.: Радио и связь, 2000, 384 с.
5. Радько Н.М., Козленко Н.И. Адаптивная радиолиния с псевдослучайной перестройкой рабочей частоты // Радиотехника, 2010, №11. С. 23-28.
6. Хвостунов Ю.С. Использование частотного ресурса при применении адаптивной системы декаметровой связи с полнодиапазонной ППРЧ АПС «Ладога» / Региональная информатика (РИ-2012). Юбилейая Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: // Труды конференции \ СПОИСУ. – СПб, 2012. С. 212-215
7. Bazar T., Wu Y. A Complete Characterization of Minimax and Maximin Encode-Decoder Policies for Communication Channels with Incomplete Statistical Description // IEEE Trans. Inform. Theory. 1985. V. 31. №4. P. 482-489.
8. Cahn СИ Performance of Digital Matched Filter Correlator with Unknown Interference // IEEE Trans. Commun. 1971. V. 19. №6. P. 1163-1172.
9. Жодзишский М.И. Применение теории игр к синтезу оптимальной системы посимвольной передачи информации // Радиотехника. 1982. № 11. С. 77-81.
10. Чудное А.М. О минимаксных алгоритмах формирования и приема сигналов // Пробл. передачи информ. 1986. Т. 22. №4. С. 49-54.
11. Чудное А.М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Пробл. передачи информ. 1991. Т. 27. № 3. С. 57-65.
12. Чуднов А.М. Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. Л.: ВАС. 1896.
13. Комарович В Ф, Романенко Г. В. КВ радиосвязь Состояние и направления развития// Зарубежная радиоэлектроника. 1990 , №12. С 3-16.
14. Урясьев С.П. Адаптивные алгоритмы стохастической оптимизации и теории игр / Под ред. Ю.М. Ермольева. – М.: Наука, 1990.
15. Воробьев Н.Н. Основы теории игр. Бескоалиционные игры. М.: Наука, 1984.
16. Чудное А. М. Анализ систем в структурно неопределенных условиях // Изв. вузов. Радиоэлектроника, 1983, т. 26, № 3, С. 17-20.
17. Крейн М.Г., Нудельман А.А. Проблема моментов Маркова и экстремальные задачи. М.: Наука, 1973.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 681.3

ОПТИМАЛЬНОЕ РЕЗЕРВИРОВАНИЕ ОТКАЗОУСТОЙЧИВОЙ ДРЕВОВИДНОЙ СЕТИ

Богатырев Владимир Анатольевич[1], Богатырев Анатолий Владимирович[2],
Богатырев Станислав Владимирович[3],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
[2,3]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, д. 49,
e-mail: vladimir.bogatyrev@gmail.com

Аннотация: Приводится методика построения структуры отказоустойчивой многоуровневой сети древовидной топологии. Предлагаемая методика основывается на решение оптимизационной задачи с минимизацией затрат на проектирование, реализацию и эксплуатацию подобных сетей.

Ключевые слова: *корпоративная сеть; топология сети; оптимизация структуры сети; отказоустойчивость; надежность; резервирование; методика построения сети.*

OPTIMAL REDUNDANCY OF FAULT-TOLERANT NETWORK TREE TOPOLOGY

Bogatyrev Vladimir [1], Bogatyrev Anatoly [2], Bogatyrev Stanislav[3],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2,3] St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverkskiy av. 49,
e-mail: vladimir.bogatyrev@gmail.com.

Abstract: The method of construction of structure failover multi-level network tree topology. The proposed method is based on solution of optimization problems with minimization of expenses on design, implementation and operation of such networks.

Keywords: *the corporate network; the topology of the network; optimizing the structure of the network; fault tolerance, reliability; redundancy; a method of constructing network.*

Введение. Информационно-экономическая безопасность корпораций определяется отказоустойчивостью и надежностью телекоммуникационных систем, которые, как правило, имеют многоуровневую древовидную структуру, с резервированием коммуникационных узлов и их связей [1-4]. Ограниченность ресурсов на построение сети и требования высокой надежности и производительности обусловливают потребность решения задачи оптимизации коммутационной системы. Оптимизация многоуровневой резервированной коммуникационной системы связана с необходимостью учета роста стоимости и снижения надежности коммутационных узлов при увеличении числа их портов и связей, в результате увеличения кратности резервирования выше и нижерасположенных узлов.

Перспективы развития систем и сетей корпораций, предоставляющих информационные услуги, связаны с архитектурой SONA (Service-Oriented Network Architecture), которая создавалась специально как сетевая архитектура, ориентированная на предоставление услуг [4, 5].

В центрах обработки данных (ЦОД), соответствующих архитектуре SONA, выделяются: уровень агрегирования; внешний уровень; уровень приложений; внутренний уровень; уровень хранилищ [1,2]. Уровень агрегирования (Aggregation Layer) состоит из компонентов сетевой инфраструктуры, поддерживающих работоспособность основных сервисов, общую систему безопасности и централизованное управление системой. Внешний уровень (Front-End Layer) - содержит Web, SMTP, FTP- серверы. Уровень приложений (Application Layer) поддерживает приложения, отвечающие за деятельность предприятия (серверы приложений). Внутренний уровень (Back-End Layer) обеспечивает функционирование центральных баз данных (серверы баз данных). Уровень хранилищ

(Storage Layer)- представляет инфраструктуру хранения данных. Межуровневое взаимодействие осуществляется через коммуникационные узлы.

Для обеспечения высокой надежности, отказоустойчивости и производительности узлы каждого уровня и связывающие их коммуникационные средства, резервируются [6-8].

При многоуровневой архитектуре ЦОД задача оптимизации системы сводится к определению кратности резервирования компьютерных и коммуникационных узлов каждого уровня, при котором техническая эффективность системы максимальна, а затраты на ее реализацию не превышают допустимый предел.

Постановка задачи. Рассмотрим трехуровневую сеть, характерную для построения корпоративных сетей [1-4]. Коммутаторы нижнего уровня (КНУ) выполняют функции уровня доступа, коммутационные узлы среднего уровня (КСУ) - уровня распределения, а коммутаторы верхнего уровня (КВУ) – уровня ядра сети. Базовая структура сети без резервирования коммутационных узлов определяется числом коммутационных узлов среднего уровня M_1, подключаемых к узлам верхнего уровня, и числом узлов нижнего уровня M_2, подключаемых к узлам среднего уровня. Для обеспечения отказоустойчивости сети коммутационные узлы каждого уровня базовой сети резервируются.

Увеличение кратности резервирования узлов приводит к техническому противоречию, так с одной стороны оно потенциально связано с увеличением надежности всей системы, а с другой - с усложнением коммутационных узлов и, как следствие, со снижением их надежности, что отрицательно сказывается на надежности всей системы. Кроме того увеличение кратности резервирование узлов приводит к возрастанию стоимости системы в результате увеличения не только числа, но и стоимости коммутационных узлов из-за увеличения числа их портов и связей.

Разрешение рассмотренного противоречия требует поиска оптимальной кратности резервирования коммутационных узлов, при которой достигается максимум надежности системы и минимум задержек передаваемых данных при ограничении средств на ее построение.

В результате оптимизации кратности резервирования коммутационных узлов формируется трехуровневая структура отказоустойчивой трехуровневой сети, представленная на рис. 1.

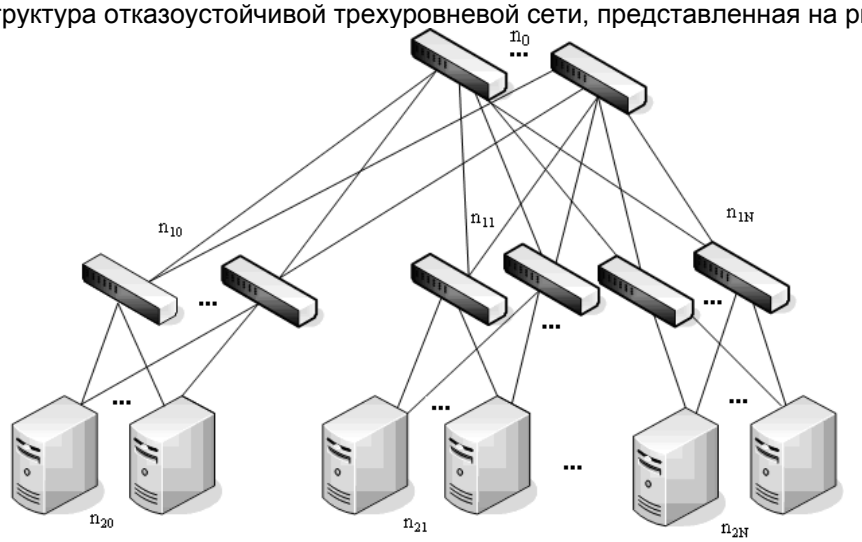


Рис.1. Структура отказоустойчивой сети

Оптимальное проектирование многоуровневых резервированных сетей возможно в одной из нижеприведенных постановок.

Для трехуровневых (M=3) сетевых структур при первой постановке оптимизации требуется найти число (кратность резервирования) узлов на каждом уровне $n=(n_0,n_1,...,n_M)$, при котором достигается максимум надежности системы, минимум среднего времени пребывания запросов в системе, при ограничении стоимости реализации системы:

$$P(n)\to\max \quad \text{и} \quad T(n)\to\min, \text{ при } C(n)=\sum_{i=1}^{M}c_i n_i \le C_0 .$$

При второй постановке задачи оптимизации требуется найти кратность резервирования узлов на каждом уровне, при котором обеспечивается минимум стоимости реализации:

$$C(n)=\sum_{i=1}^{M}c_i n_i \to\min, \quad \text{при } P(n)\ge P_0, \quad T(n)\le T_0 .$$

При этом T_0 ,P_0 ,C_0 – предельно допустимые значения среднего времени ожидания, надежности и стоимости системы.

При оптимизации структуры сети, будем считать заданными интенсивность входного потока запросов λ, множество возможных вариантов построения (выбора) узлов каждого уровня, причем i-й

вариант характеризуется вектором параметров: среднего времени выполнения запросов, надежности и стоимости реализации (v_i, p_i, c_i). На каждом уровне используются однотипные узлы.

Поставленная задача оптимизации является векторной, сложность которой обусловлена тем, что одно решение (альтернатива) может доминировать по одним показателям и уступать по другим. В задачах принятия решений по векторному показателю важен выбор решающего правила, основанного на компромиссе между значениями компонент векторного показателя.

При оптимизации сети проводится поиск кратности резервирования и типов коммуникационных узлов, выбираемых из некоторого множества доступных вариантов их реализации.

Методика построения структуры сети. Поиск оптимального построения коммуникационной системы, основанный на переборе возможных комбинаций типов коммутационных узлов различных уровней, включает:

1. Формирование критерия оптимизации многоуровневой сети и ограничений по частным показателям.
2. Формирование вектора частных показателей эффективности для коммуникационных средств каждого уровня.
3. Формирование множества вариантов базовых коммутационных узлов, которые могут быть использованы на каждом уровне сети (например, на основе морфологического анализа).
4. Определение области Парето для вариантов коммуникационных узлов каждого уровня. Для s-го уровня i-й вариант, представленный вектором $\left(p_{is}, v_{is}, c_{is}\right)$, доминирует по Парето над j-м вариантом, $\left(p_{js}, v_{js}, c_{js}\right)$, если выполняется условие:

$$\left[\left(p_{is} \geq p_{js}\right) \wedge (v_{is} \leq v_{js}) \wedge (c_{is} \leq c_{js})\right] \wedge \left[\left(p_{is} > p_{js}\right) \vee (v_{is} < v_{js}) \vee (c_{is} < c_{js})\right].$$

5. Построение моделей для оценки исследуемой сетевой структуры по частным показателям (надежность стоимость, время ожидания запросов).
6. Определение комплексного критерия эффективности многоуровневой сети, объединяющего частные показатели качества системы.
7. Комбинаторный выбор (перебор) из множества Парето (множества эффективных решений) вариантов коммутационных узлов совместно используемых, на различных уровнях синтезируемой сети.
8. Определение для каждого варианта выбранных узлов при заданной базовой структуре сети кратности резервирования узлов, обеспечивающей максимум (минимум) критерия оптимизации при выполнении заданных ограничений.
9. Сравнение показателя эффективности формируемой структуры с показателем эффективности структуры, ранее определенной как наилучшей (в начале, как наилучшая задается базовая структура). Если показатель качества вновь сформированной структуры лучше, то она определяется как наилучшая.
10. Если перебор всех комбинации реализации узлов разных уровней не закончен, то переходим к выполнению п.5, если закончен, то в качестве оптимальной реализации многоуровневой сети выбираем последнюю структуру, определенную как наилучшую.
11. Вычисление значений частных показателей при определенной в результате оптимизации кратности резервирования коммутационных узлов на каждом уровне.
12. Анализ полученных результатов и при необходимости изменение налагаемых ограничений на технические и стоимостные показатели и повторение процедуры оптимизации.

При выполнении пункта 7 возможна модификация, при которой в результате оптимизации ищется не только кратность резервирования коммутационных узлов, но и базовая топология сети, включая определение параметров M1 и M2.

В результате оптимизации определяются типы коммутационных узлов и кратность их резервирования на различных уровнях.

Рассмотрим формирование минимальной по стоимости базовой трехуровневой древовидной сети при выборе коммуникационных узлов, из некоторого множества, заданного для каждого уровня сети.

Будем считать заданными общее число M компьютерных узлов, подключаемых к сети и варианты коммутационных узлов, используемых на каждом уровне сети, различающиеся числом портов и стоимостью.

Поиск оптимальной конфигурации сети включает перебор типов коммутационных узлов, используемых на верхнем уровне сети, с определением для каждого из них всевозможных комбинаций типов коммутационных узлов, используемых на двух нижерасположенных уровнях.

При выборе каждого типа коммутационных узлов верхнего уровня в результате перебора типов коммутационных узлов, используемых на нижнем уровне, для каждого i-го варианта находим число коммутационных узлов m0i , необходимое для подключения к сети всех M компьютеров. Результат

представляем вектором (m0i). После чего находим число узлов на среднем уровне, необходимое для связанности системы, при всевозможных комбинациях типов узлов на нижнем и среднем уровне. Результат представляем матрицей $\left\| m1_{ij} \right\|$, элемент которой m1ij равен числу коммутационных узлов j-го типа на среднем уровне при использовании i-го типа узлов на нижнем уровне. Искомое число коммуникационных узлов вычисляется как:

$$m0_i = ceil\left(M/(r_i - 1)\right),\ m1_{ij} = ceil\left[ceil(M/(r_i - 1))/(r_j - 1)\right],$$

вектор r задает варианты коммуникационных узлов по числу портов (ceil(z) – число не меньшее z).

Определив число коммутационных узлов различного типа, требуемых для связанности системы, найдем стоимость коммуникационной системы для каждого варианта комплектации коммуникационных узлов на нижнем и среднем уровнях при k-ом типе узлов на верхнем уровне, как $c_{ij} = c_i m0_i + c1_j m1_{ij} + c2_k ceil\left(m1_{ij}/(r_k - 1)\right)$. Векторы c, c1, c2 задают стоимости коммутационных узлов с соответствующим числом портов, применяемых на различных уровнях сети.

Результаты расчета стоимости системы для всех комбинаций типов коммутационных узлов на двух нижних уровнях (при k-ом типе узлов на верхнем уровне) представим матрицей C.

Найдем наименьший элемент матрицы C, соответствующий минимальной стоимости системы, при выбранном k-ом типе узлов верхнего уровня, найденное значение стоимости внесем в качестве k-го элемента вектора (a).

Повторяя описанную процедуру при всех значениях k, сформируем вектор (a), минимальный элемент которого и будет соответствовать минимальной стоимости реализации трехуровневой коммутационной системы при заданном ряде используемых коммутационных узлов, различающихся по числу портов и стоимости.

После чего по соответствующей матрице C находим тип коммуникационных узлов, используемых на среднем и нижнем уровнях коммуникационной системы.

Приведенные алгоритмы позволяют из заданного ряда коммутационных узлов, различающихся стоимостью и числом портов, определить число и типы, коммутационных узлов, использование которых на различных уровнях древовидной топологии, обеспечивает минимизацию затрат на построение многоуровневой коммуникационной системы.

Заключение. Проведенные исследования могут использоваться при оптимизации структуры отказоустойчивых многоуровневых сетей, древовидной топологии. Следует отметить, что предлагаемая методика построения сетевой структуры, основывается на решение оптимизационной задачи, что особенно актуально в условиях, когда остро стоит проблема построения технически эффективных систем при минимизации затрат на их проектирование, реализацию и эксплуатацию.

СПИСОК ЛИТЕРАТУРЫ

1. Ретана Ф. Принципы проектирования корпоративных IP-сетей. М.: Вильямс ,2002. 368 с.
2. Колбанев М.О., Татарникова Т.М., Воробьев А.И. Модель обработки клиентских запросов //Телекоммуникации. 2013. № 9. С. 42-47.
3. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель балансировки нагрузки в вычислительном кластере центра обработки данных //Информационно-управляющие системы. 2012. Т. 3. № 58. С. 37-41.
4. Архитектура и технологии ЦОД. [электронный ресурс] Режим доступа: http://www.nvisiongroup.ru/tech_cod.html, свободный.
5. Черняк Л. ЦОД в стиле SONA. [электронный ресурс]. Режим доступа: http://www.osp.ru/cw/2006/17/1155286/ , свободный.
6. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация древовидной сети с резервированием коммутационных узлов и связей //Телекоммуникации. 2013. № 2. С. 42-48.
7. Богатырев В.А., Богатырев С.В. К анализу и оптимизации серверных систем кластерной архитектуры с балансировкой нагрузки //Приборы и системы. Управление, контроль, диагностика. 2010. № 2. С. 4-9 .
8. Богатырев В.А., Богатырев С.В. Оптимизация структуры многоуровневой резервированной компьютерной системы при многовариантности потока запросов //Вестник компьютерных и информационных технологий. 2010. № 2. С 33-41.

УДК 004.056.53

ПЕРСПЕКТИВЫ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ДЛЯ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ

Брунилин Алексей Александрович,
Военная академия связи имени Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр-т, д.3
e-mails: ale483@mail.ru

Аннотация. Статья рассматривает основные положения онтологического подхода к интеграции разнородных информационных ресурсов, лежащие в основе организации взаимодействия инфо-телекоммуникационных систем, обеспечивающих организационное управление. Дано краткое определение онтологии в информатике. Рассмотрены результаты эксперимента по отображению реляционных баз данных в онтологии, представлены выводы по их применимости на практике,

результаты эксперимента по отображению обобщены методикой. Предложена концепция онтологического похода к объединению гетерогенных инфо-телекоммуникационных систем на основе гибридного способа взаимодействия онтологий. Определены направления дальнейших исследований в данной области.

***Ключевые слова**: информационная телекоммуникационная система, информационное взаимодействие, онтология, реляционная база данных, семантическая модель.*

ONTOLOGICAL APPROACH TO INFORMATION INTERACTION ORGANIZATION OF HETEROGENEOUS AUTOMATED SYSTEMS FOR SPECIAL PURPOSES

Alexey Brunilin
Military Academy of Communications
e-mails: ale483@mail.ru

Abstract. The article deals with the main provisions of the ontological approach to integrating heterogeneous information resources. These provisions are the basis of the information interaction of heterogeneous automated systems intended to provide the organizational management. A brief definition of ontology in computer science has been done. The experimental results on displaying relational databases in the ontology were considered. Conclusions on their applicability in practice were presented and currently obtained results were summarized in a common technique. The concept of ontological approach to integrate heterogeneous systems based on hybrid method of interaction of ontologies was offered. Directions for further research in this area were identified.

Keywords: *automated system, information interaction, relational database, ontology, semantic model.*

Обеспечение информационного взаимодействия разнородных инфо-телекоммуникационных систем (ИТКС) является важной и достаточно сложной задачей, на решение которой в настоящее время направлены усилия и исследования многих специалистов и разработчиков специального программного обеспечения. Решение этой задачи имеет большое практическое значение, так как с развитием информационных технологий разработчики ИТКС, стремясь максимально удовлетворить информационные потребности заказчика, внедряют всё новые и новые методы обработки данных. На практике это приводит к тому, что базы данных, среди которых до недавнего времени реляционные базы считались наиболее прагматичными, нельзя более считать единственно возможным и наиболее эффективным средством хранения и обработки данных. Так, например, всё большее распространение приобретают такие средства комплексного администрирования данных, как XML-, RDF-, NoSQL-базы данных, а также комплексные хранилища, сочетающие перечисленные, «классические» реляционные и другие типы баз данных [1], [2].

Кроме того, в различных отраслях человеческой деятельности используются не комплексные автоматизированные системы (универсальные моно-системы, являющиеся законченными программно-аппаратными комплексами), создающие единую информационную среду производства и управления отрасли, а более дешёвые в разработке и эксплуатации комплексы узкопрофильных ИТКС.

Однако проблема взаимодействия ИТКС отчётливо видна даже с учетом абсолютных достоинств реализации идеи дробления автоматизированных систем по функциональному предназначению.

На практике в большинстве случаев разработкой профильных ИТКС могут заниматься независимые предприятия-разработчики. Поэтому добиться полной унификации стандартов и протоколов обмена данными зачастую не представляется возможным. Тем не менее, при управлении отраслевым проектом лицу, принимающему решение, или руководящему органу для выработки управляющих воздействий необходимо опираться на результаты комплексного анализа разнородной информации. В данных обстоятельствах мы говорим об одном из случаев отчётливого проявления проблемы, аналогичной широко известной проблеме «последней мили» - курьёзной ситуации, когда предварительная отраслевая информация обрабатывается и анализируется в автоматическом или автоматизированном режиме, а наиболее важный итоговый этап комплексного анализа полученных данных для выработки предложений на принятие решений – «ручным» способом.

Подобное положение дел негативно сказывается на оперативности и адекватности принятия решений, что приобретает важное значение при применении комплексов ИТКС специального назначения в реальных условиях. Под данными комплексами понимаются системы средств автоматизации и ИТКС, задействованные для принятия решений при возникновении чрезвычайных ситуаций, функционирующие в интересах силовых ведомств и иных критических инфраструктур [3].

В качестве возможного подхода к решению указанной проблемы предлагается создание универсальной информационно-аналитической структуры, программная платформа которой предоставляла бы пользователю (то есть потребителю информационной услуги) возможность доступа к разнородной информации и даже к результатам её предварительного машинного анализа

безотносительно к её природе, способам хранения и обработки. Указанные свойства данной информационной платформы позволяют предложить новый подход к организации взаимодействия ИТКС, основанный на использовании особой разновидности баз знаний, называемой онтологией.

Термин «онтология» заимствован из гуманитарных наук, где он традиционно понимается как раздел философии, изучающий бытие, «всё сущее». Позже под онтологией стали понимать результат классификации, систематизацию знаний в различных предметных областях.

На сегодняшний день онтологии выступают в качестве наиболее современного, универсального способа описания, моделирования знаний об окружающем мире, имеющего максимальные выразительную силу и возможность производить автоматизированные рассуждения.

В информатике под «онтологией» понимается представление предметной области (domain of interests) в виде взаимосвязанных понятий (индивидов). В основу программной реализации онтологий положены принципы объектно-ориентированного подхода (ООП). Так, для установления общности индивидов используются классы, определяемые как наборы абстрактных свойств. Классы в соответствии с ООП могут иметь подклассы, наследующие свойства родительского класса и добавляющие собственные. Индивид, принадлежащий классу, обладает всем набором свойств данного класса; любой индивид может быть представителем нескольких классов. Свойства в онтологической модели рассматриваются как связи между индивидами.

В качестве базовой информационной единицы онтологии выступает так называемый «RDF-триплет» (RDF – Resource Description Framework, триплет – набор информационных сущностей «объект-предикат-субъект»). Предметная область, описанная таким способом, обладает компьютерной семантикой, то есть возможностью устанавливать и обрабатывать смысловые отношения между понятиями с помощью вычислительных машин.

Компьютерная семантика раскрывается математическим аппаратом дискрипционных логик (например, EL-логики), который является развитием стандартной семантики Тарского (логики первого порядка). К достоинствам EL-логики можно отнести достаточную для обработки машинных суждений выразительность, а также сходимость вычислительных алгоритмов за конечное (обычно – полиномиальное) количество итераций [4]. Указанные свойства обеспечивают возможность формирования и обработки запросов к онтологиям на основе программного механизма логического вывода [4], [5].

Суть онтологического подхода при решении проблемы организации информационного взаимодействия разнородных ИТКС заключается в создании универсальных, кроссплатформенных информационных структур, использующих семантические метаописания данных, как собственных, так и надстроек к уже существующим разнородным информационным массивам, в том числе к базам данных различных архитектур.

Программные комплексы разработки онтологий обладают возможностью создания процедур логического вывода, то есть получения машинным способом новых (неявных) знаний на основании имеющихся (установленных, уже доказанных) фактов и отношений между ними. Это позволяет автоматизировать процедуры семантического (смыслового) анализа имеющейся информации и даёт возможность выработки предварительных рекомендаций на принятие управляющих решений.

Одним из основных достоинств онтологического подхода можно определить возможность как априорного, так и апостериорного анализа принятых решений, что даёт возможность постоянно расширять базу логического вывода онтологии. Это позволяет накапливать, систематизировать и, главное, предлагать в автоматизированном режиме наиболее эффективные управленческие воздействия для решения информационных задач.

Об актуальности использования онтологий в качестве информационной платформы для решения проблемы взаимодействия ИТКС свидетельствует в том числе тот факт, что на сегодняшний день консорциумом развития глобальной сети (W3C – World Wide Web Consortium) уже стандартизованы не только несколько языков разработки онтологий – OWL (Web Ontology Language) в трёх модификациях [6] и SWRL (Semantic Web Rule Language) [7], – но и спецификации языков отображения реляционных баз данных в онтологии DM (Direct Mapping) и R2RML (Relational DataBase to Resource Description Framework Mapping Language) [8].

Для практической апробации предлагаемого подхода используем методику создания и использования онтологии для интеграции реляционных баз данных, предложенную в работе [9]. В данной работе на примере информационного объединения двух удалённых друг от друга и работающих под управлением разных СУБД баз данных демонстрируется результативность онтологического подхода. Несмотря на то, что создание запросов к разным реляционным базам данных само по себе не является технически сложной задачей, практическая реализация механизма интеграции разнородных реляционных баз данных посредствам отображения их в онтологические конструкции демонстрирует жизнеспособность данного подхода. При этом следует отметить, что применение для указанных целей онтологического подхода даёт возможность интеграции разнородных информационных ресурсов, включая нереляционные базы данных.

Попытка интеграции информационных ресурсов показала, что объединение даже реляционных сущностей под управлением различных СУБД (в эксперименте использовались базы данных,

созданные в MySQL и Линтер-ВС под управлением Microsoft Windows-7 и МСВС-3.0 соответственно), связано с решением ряда практических вопросов. Выяснилось, что даже при наличии программного доступа из внешней оболочки к обеим базам данных (например, через сервис ODBC – Open DataBase Connectivity, JDBC – Java DBC, и им подобные) использовать часть языковых конструкций языка SQL (Structured Query Language) в привычном виде не представляется возможным, так как. разработчики систем управления баз данных используют в качестве средства манипуляции данными так называемые «SQL-диалекты» – упрощённые версии стандартизованного языка структурированных запросов к базам данных. Это ограничение лишает конечного разработчика возможности в полной мере использовать выразительность и мощь классического SQL при создании внешних запросов к базам данных.

В конечном итоге задача объединения может быть решена выполнением дополнительных шагов, например, дроблением исходных запросов на более простые. Однако универсальная применимость этого способа вызывает сомнения, т.к. для реальной работы с данными обоих ресурсов необходимо производить дополнительные действия по агрегированию и анализу полученных промежуточных результатов. Это, очевидно, влечёт увеличение суммарного времени выполнения запросов, а также усложняет процесс разработки пользовательского интерфейса, ставя вопрос о предоставлении пользователю возможности создавать произвольные запросы на грань практической разрешимости.

Иные способы объединения, такие, как полное/частичное перекачивание данных под управление единой СУБД, или обработка информационных массивов «налету» средствами программной оболочки (не через интерфейс СУБД), также могут дать положительный результат. Однако, принимая во внимание затраты на обеспечение совместимости данных, полная потеря связи с источником в первом случае и сложность, уникальность способов программной реализации во втором случае не позволяют говорить о широкой применимости данных методов на практике.

В отличие от описанного выше метода прямого связывания реляционных баз данных, объединение их посредством онтологий в практическом опыте, аналогичном описанному в [9], не вызывает существенных проблем. Создание массивов данных, полученных из различных реляционных источников при помощи упомянутых выше языков отображения DM или R2RML, происходит в виде накопления RDF-триплетов. Объединение полученных массивов осуществляется обычным добавлением между соответствующими информационными сущностями связи типа rdfs:SubClassOf или owl:EquivalentClass, после чего обращение к полученным онтологиям (например, формирование запросов с использованием языка SPARQL) осуществляется без ограничений, как к единому информационному массиву.

Ограничением в области применимости отображения реляционных баз данных в онтологию выступает нечувствительность получаемой информационной структуры к изменениям данных, производимых над источником. Соответственно, применение данного метода видится целесообразным в системах со стабильной, не интенсивно обновляемой структурой и данными (словари, классификаторы и т.п.), либо в системах с малым объёмом вырабатываемой информации (например, комплексы периодически опрашиваемых внешних источников информации об обстановке).

Также необходимо иметь в виду, что ограничения на установление связей в онтологиях существенно более мягкие, чем в реляционных базах данных. Таким образом, объединение онтологий в условиях недостаточно точного инфологического анализа их структуры увеличивает вероятность установления ошибочных связей. Это обстоятельство способно привести к нежелательным вычислительным последствиям, что может выражаться в нарушении семантической связности понятий и классов, и, тем самым, не позволит считать онтологическую модель описания предметной области информационной задачи адекватной.

В качестве недостатка данного метода следует отметить более низкую производительность вычислений над онтологиями по сравнению с вычислениями в реляционных СУБД.

Несмотря на ряд ограничений и недостатков метода отображения реляционных БД в онтологии с точки зрения организации взаимодействия ИТКС с использованием семантического моделирования, полученные результаты свидетельствуют о возможности практической реализации подобного отображения для решения более узких задач, как например смена модели данных информационной задачи при переходе проекта на онтологическую платформу, внедрение механизмов семантического поиска и некоторых других задач. Эксперимент позволяет обобщить полученный в ходе работы практический опыт методикой отображения объектов реляционных баз данных в онтологическую модель.

Предлагаемая методика имеет следующие этапы:

a) подготовительный этап:
   1) анализ предметной области;
   2) выявление главных информационных задач;
   3) определение исходных данных, ограничений;
   4) выбор типа онтологического взаимодействия;

b) перевод информационных сущностей исходных БД в термины онтологий:

1) уточнение запросов на преобразование данных;
2) непосредственно извлечение и представление данных в терминах онтологий;
3) использование процедур логического вывода для выявления отношений между объектами онтологии;

c) объединение онтологий;
d) адаптация онтологий для решения поставленных информационных задач.

На практике для объединения нескольких ИТКС необходимо использовать другие преимущества онтологий. В частности, несомненным достоинством применения семантического подхода как интегрирующего инструмента для разнородных ИТКС, видится возможность надстраивать онтологию над уже разработанными информационными комплексами. По сравнению с затратами на создание «единой АСУ отрасли», онтологический подход позволяет в значительной степени удешевить и ускорить процесс разработки программного комплекса, работа которого также направлена на поддержку принятия решения, исходя из анализа разнородной информации.

На рисунке 1 представлен вариант концептуальной схемы применения онтологий для организации взаимодействия ИТКС.

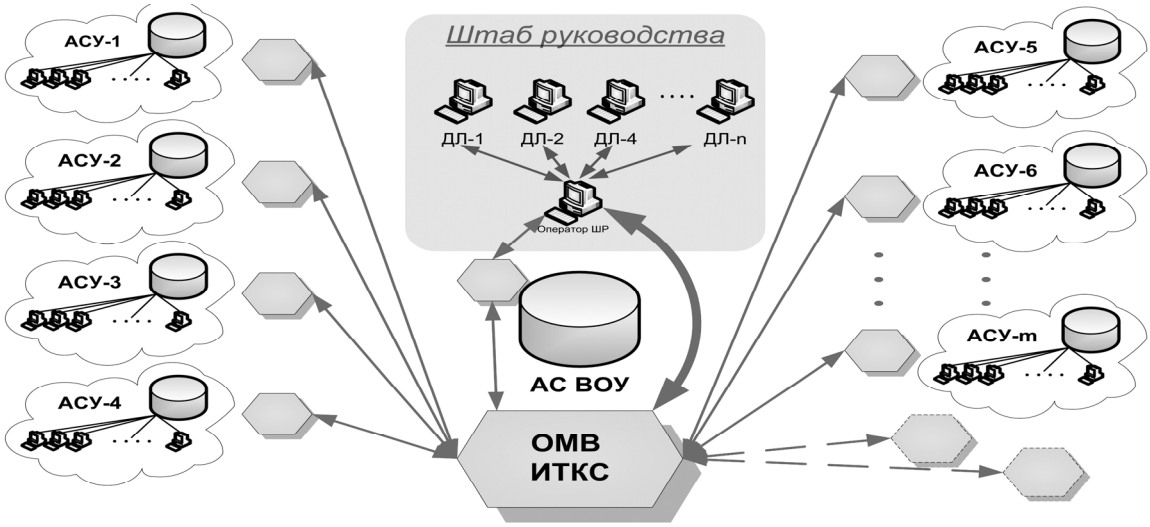


Рис. 1. Схема применения онтологий для организации взаимодействия ИТКС

Для каждой отраслевой ИТКС (АСУ) создаётся онтологическая модель предметной области. При этом если известны схемы информационных потоков не только по горизонтали (внутри организации) но и по вертикали (автоматизированные системы вышестоящих и нижестоящих органов управления), то и их онтологические модели могут быть созданы аналогичным способом. Подобная универсальность позволит заблаговременно с минимальными затратами создавать модели для ИТКС, планируемых к подключению для работы в совместных (например, межведомственных) проектах.

Для объединения онтологий в данном случае используется более естественный для XML-конструкций способ включения, представляющий собой указание URI (Unique Resource Identifier) соответствующей онтологии в качестве параметра rdf:resource тэга <owl:>, например:

```
<owl:Ontology rdf:about="АСУ-1">
    ...
    <owl:imports rdf:resource="http://www./.../.ASU-1.ru/root"/>
    ...
</owl:Ontology>
```

При последующих обращениях допустимо ссылаться на ресурсы соответствующей онтологии при помощи указания её псевдонима [6].

В описываемом проекте реализуется гибридный способ взаимодействия онтологий, который подразумевает следующее: каждой из m отраслевых ИТКС соответствует собственная онтологическая модель описания их предметных областей (рассматривается внутренний уровень взаимодействия, ИТКС организации). При достаточно большом количестве связываемых систем логично избегать варианта создания внутри каждой отдельной онтологии описаний для остальных взаимодействующих с ней систем. В пределе их количество равно $(m-1)$. Это может привести к необходимости создания $m \times (m-1)$ программных описаний взаимодействия, что будет нерациональным и с позиций разработки, и с точки зрения использования вычислительных ресурсов в ходе эксплуатации. Для того чтобы избежать подобной ситуации, создаётся ещё одна $(m+1)$-я

онтологическая модель, которая будет объединять их и описывать в терминах дескриптивной логики механизмы логического вывода (взаимодействия) автоматизированных систем.

Онтологический подход при организации взаимодействия упрощает процедуру общения пользователя (оператора) с информационной средой, в особенности оператора средств автоматизации руководящего звена, имеющего в качестве основной цели анализ предварительно обработанной разнородной информации. Данное преимущество определяется природой онтологической модели, унифицирующей порядок доступа к данным, циркулирующим в различных ИТКС, безотносительно к способам выработки этих данных и их природе. В свою очередь, наличие унифицированной возможности запрашивать результаты обработки данных любой ИТКС организации создаёт реальные предпосылки для частичной автоматизации процесса комплексного информационного анализа, являющегося основой для выработки предложений на принятие генеральных управляющих воздействий. До настоящего времени именно этот этап принятия решений осуществлялся исключительно в «ручном» режиме.

Необходимо отметить, что онтологическое моделирование предметной области даёт возможность пользователю формировать запросы к системе, позволяя ожидать наилучших результатов по их релевантности [5], что на текущем этапе развития информационных технологий является одним из параметров, определяющих эффективность ИТКС. Результативность поиска в данном случае обеспечивается программным механизмом семантического поиска.

Дальнейшими шагами в исследовании онтологического подхода к объединению разнородных ИТКС представляются:

– практическая отработка объединения нереляционных баз данных;

– создание программ-администраторов, «отвечающих» за информационное (функциональное) направление (обслуживание информационной задачи) и «общающихся» между собой в рамках достижения главной информационной цели;

– разработка глобальных отраслевых онтологий с возможностью их дальнейшего использования в качестве опорных универсальных таксономий и классификаторов.

Таким образом, применение онтологического подхода для организации взаимодействия разнородных инфо-телекоммуникационных систем имеет серьёзные практические перспективы и требует дальнейшей всесторонней разработки.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. – 2013. – Вып. 2 (25). – С.113–134.
2. Полубелова О.В., Котенко И.В., Саенко И.Б. Онтологический подход к построению интеллектуальных сервисов хранения и обработки событий безопасности // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'12». Научное издание в 4-х томах. – М.: Физматлит, 2012. – Т. 2. – С. 394–399.
3. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1 (24). С.21–40
4. Конев Б.Ю. Онтология и представление знаний. – http://www.lektorium.tv/speaker/2680 [Request date: 30.11.2014].
5. T. Berners-Lee, J. Hendler, and O. Lassila. The Semantic Web. Scientific American, 284(5):34-43, 2001. – http://ezolin.pisem.net/logic/semantic_web_rus.html [Request date: 10.11.2014].
6. OWL 2 Web Ontology Language Document Overview (Second Edition). W3C Recommendation 11 December 2012. – http://www.w3.org/TR/owl2-overview [Request date: 30.11.2014].
7. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission 21 May 2004. – http://www.w3.org/Submission/SWRL [Request date: 30.11.2014].
8. R2RML: RDB to RDF Mapping Language. W3C Proposed Recommendation 14 August 2012. – http://www.w3.org/TR/2012/PR-r2rml-20120814 [Request date: 30.11.2014].
9. Колесов А.О., Наместников А.М. Интеграция реляционных данных на основе онтологического подхода // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, Казань, Россия): Труды конференции. Т.3. – Казань: Изд-во РИЦ «Школа». – 2014. – С. 146–154.

УДК 004.75

МНОГОКРИТЕРИАЛЬНЫЙ ВЫБОР СТРУКТУРЫ ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Верзун Наталья Аркадьевна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mail: dina_25@hotbox.ru.

Аннотация: Рассмотрена задача многокритериального выбора множества вариантов построения неоднородной локальной сети, состоящей из двух подсетей передачи: данных и непрерывной информации. Предложена двухэтапная процедура выбора на основе множеств Парето и представлен пример её использования.

Ключевые слова: *многокритериальный выбор; неоднородная локальная сеть; вероятностно-временные характеристики; стоимостные характеристики; множество Парето.*

MULTICRITERIA CHOICE LAN STRUCTURE COMPANY

Verzun Natalia,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: dina_25@hotbox.ru.

Abstract: The problem of multicriteria choice multiple options for building heterogeneous network consisting of two subnetworks transfer: data and continuous information. Proposed a two-stage choice procedure based on Pareto sets and an example of its use.

Keywords: *multicriteria choice; heterogeneous LAN; probability-temporal characteristics; cost characteristics; Pareto set.*

Введение. Функционирование современного предприятия базируется на применении информационных технологий. Внедрение и использование в бизнесе таких средств как электронные платежи, безбумажный документооборот и пр., ведет к тому, что каждый сбой в работе компьютерной сети предприятия может нанести не только “моральный” ущерб, но иповлечь за собой ощутимые “материальные” потери[1],[2]. Поэтому, как припроектировании и создании компьютерной сети, так и при её расширении имодернизации необходим взвешенный подход к выбору структуры сети[3].

В данной работе рассматривается задача многокритериального выбора множества вариантов построения неоднородной локальной сети. Предполагается, что сеть состоит из *j* подсетей($j = \overline{1,J}$). Каждая подсеть предназначенадля передачи информации определенного типа.

1.Критерии выбора. Коммуникационные системы станций сети моделируются СМО $M^{д}/G^{д}/1$. Математические модели различных вариантов построения сети[4],[,5] позволяют найти следующие вероятностные и вероятностно временные характеристики подсетей. Среднее время задержки пакетов *j*-го типа

$$\overline{t_{qj}} = T_{окj}\overline{n_{qj}}; \overline{n_{qj}} = (d/dz^{-1})\, f_{qj}(z)\Big|_{z=1}; j = \overline{1,J}, \qquad (1)$$

где $f_{qj}(z)$ –*z*-преобразование ряда распределения времени задержкиинформации *j*-го типа[4],[5]. Вероятность своевременной доставки пакетов *j*–го типа

$$\overline{\Pi_{qj}} = f_{qj}(z)\Big|_{z=Q_{дj}^{-1}}; Q_{д} = 1 - \frac{T_{ок}}{\overline{T_{дj}}}; j = \overline{1,J}, \qquad (2)$$

где $T_{ок}$– интервал дискретного времени, $\overline{T_{дj}}$ – среднее допустимое время старения для *j*–го типа информации. Вероятность потерь пакетов *j*–го типа

$$\Pi_j = 1 - Q_{cj}\overline{\Pi_{qj}}; j = \overline{1,J}, \qquad (3)$$

где Q_{cj} – вероятность успешной передачи пакета *j*–го типаопределяется следующим образом

$$Q_{cj} = (1-p)^{n_{кj}}; j = \overline{1,J},$$

$$n_{кj} = r_{aj} + r_{у} + k_j + r_{к}; r_{aj} = 2\log_2 N_j,$$

где p – вероятность ошибки в среде передачи, N_j – число станций *j*–ой подсети, $r_{у}$ – длина поля управления, $r_{к}$ – число контрольных разрядов, k_j – длина информационной части кадра *j*–го типа.

В качестве стоимостной характеристики неоднородной локальной сети предлагается использовать прибыль от её эксплуатации

$$\Pi_{р} = Д - К - \sum_{t=1}^{T_{ок}} Э_{г}, \qquad (4)$$

где $Э_{г}$ – годовые эксплуатационные расходы, включают в себя материальные затраты на содержание и обслуживание сети, а также заработную плату обслуживающему персоналу, $К$ – единовременные капитальные вложения, связанные с введением в строй сети, $Д$ – доход(финансовые поступления от деятельности предприятия), $T_{ок}$ – срок окупаемости сети(в годах).

2.Этапы выбора структуры. Выбор осуществляется в два этапа. На первом этапе многокритериальный выбор множества вариантов, используя принцип декомпозиции, разбивается на j процедур (где j –количество подсетей в сети), относительно прибыли от эксплуатации($\Pi_{р}$) и

среднего времени задержки j-ой подсети($\overline{t_{qj}}$) , используя отношения Парето. Для каждой подсети j , находится множество Парето

$$C_j^P(W') = \arg\max_{w\in W'} \Pi_{\text{р}}(w), C_j^P(W') = \arg\min_{w\in W'} \overline{t_{qj}}(w), j=\overline{1,J}, \qquad (5)$$

при ограничениях

$$\overline{\Pi_{qj}}(w)_{w\in W'} \geq \overline{\Pi_{qj\text{д}}}, \quad \Pi_j(w)_{w\in W'} \leq \Pi_{j\text{д}}, j=\overline{1,J}$$

где $\overline{\Pi_{qj}}$ – вероятность своевременной доставки пакетов*j*-го типа, Π_j – вероятность потерь пакетов *j*-го типа, $\overline{\Pi_{qj\text{д}}}$ и $\Pi_{j\text{д}}$ – допустимые значения вероятностей своевременной доставки и потерь пакетов*j*-го типа. На втором этапе осуществляется объединение решений двухкритериальных выборов, произведенных на первом этапе, для получения окончательного решения $C(W)$. Такое объединение может быть основано на применении следующих процедур: либо операции объединения полученных для каждой подсети множеств, либо с использованием операции их пересечения.

3.Пример выбора структуры локальной сети. Рассмотрим пример выбора структуры при следующих исходных данных: сеть состоит из двух подсетей ($J=2$): подсеть передачи данных с числом станций $N_{\text{д}}=100$ и непрерывной информации(НИ) с числом станций $N_{\text{НИ}}=300$. В подсети передачи НИ возможна передача сжатой НИ с вероятностью 0,3и несжатой НИ с вероятностью 0,7. Допустимо применение следующих вариантов протоколов доступа: маркерный(МД), регулируемый маркерный(РМД), синхронно-временной(СВД). При построении сети возможно использование шинной и кольцевой топологии (длина каналов в кольце 6,0 км; в шине 5,8 км). Передающая среда может быть двух типов: витая пара и волоконно-оптический кабель(вероятность ошибки в канале связи $p=10^{-7}$). Возможные скорости передачи: 4;12;34;140 Мбит/с. На входы станций сети поступают бернуллиевские потоки пакетов данных и НИ. Интенсивность входного потока на станцию НИ: 0,55 пак/с, на станцию данных 50 пак/с. Данные и НИ передаются в пакетном виде с длиной информационной части 128 бит для данных, 256 бит для сжатой НИ и 1024 бит, для несжатой НИ. Заданы величины допустимых средних задержек $\overline{T_{\text{дНИ}}}=0{,}263$ с. – для пакетов НИ и $\overline{T_{\text{дД}}}=0{,}5$ с. – для пакетов данных. При передаче данных применяется алгоритм повышения достоверности РОС-ОЖ с бесконечным числом переспросов. НИ передается в режиме прямой связи.

Ограничения для многокритериального выбора структуры неоднородной сети(применяющей процедуры сжатия НИ): допустимая вероятность потерь пакета несжатой НИ $\Pi_{НИ}=0{,}02$, сжатой НИ $\Pi_{НЖ}=0{,}01$ допустимая вероятность своевременной доставки пакета данных: $\overline{\Pi_{q\text{дд}}}=0{,}99$, несжатой НИ $\overline{\Pi_{q\text{ннд}}}=0{,}96$,сжатой НИ $\overline{\Pi_{q\text{нжд}}}=0{,}98$.

Множество возможных вариантов построения сети включает в себя 30 вариантов и представлено в таб. 1.

Таблица 1

Множество возможных вариантов построения сети

№ вар.	1	2	3	4	5	6	7	8	9	10
Протокол доступа	Маркерный доступ									
Тип кабеля	вп	вп	св	св	св	св	св	св	св	св
Топология	ш	к	ш	ш	ш	ш	к	к	к	к
Скорость Мбит/с	4	4	4	12	34	140	4	12	34	140
№ вар.	11	12	13	14	15	16	17	18	19	20
Протокол доступа	Регулируемый маркерный доступ									
Тип кабеля	вп	вп	св	св	св	св	св	св	св	св
Топология	ш	к	ш	ш	ш	ш	к	к	к	к
Скорость Мбит/с	4	4	4	12	34	140	4	12	34	140
№ вар.	21	22	23	24	25	26	27	28	29	30
Протокол доступа	Синхронно-временной доступ									
Тип кабеля	вп	св	св	св	св	св	св	св	св	св
Топология	ш	к	ш	ш	ш	ш	к	к	к	к
Скорость Мбит/с	4	4	4	12	34	140	4	12	34	140

Обозначения: вп – витая пара, св – волоконно-оптический кабель, ш – шина, к – кольцо

После расчета характеристик по формулам (1)-(4) из предложенного к выбору множества вариантов исключены варианты, не удовлетворяющие заданным ограничениям. В результате сформировано предъявленное к выбору множество вариантов построения локальной сети:варианты 4,5,6,8,9,10,15,16,19,20. Затем многокритериальная задача выбора разбивается на три двухкритериальных (5). Отдельно для данных, несжатой НИ и сжатой НИ находим множества Парето (см. рис.1).

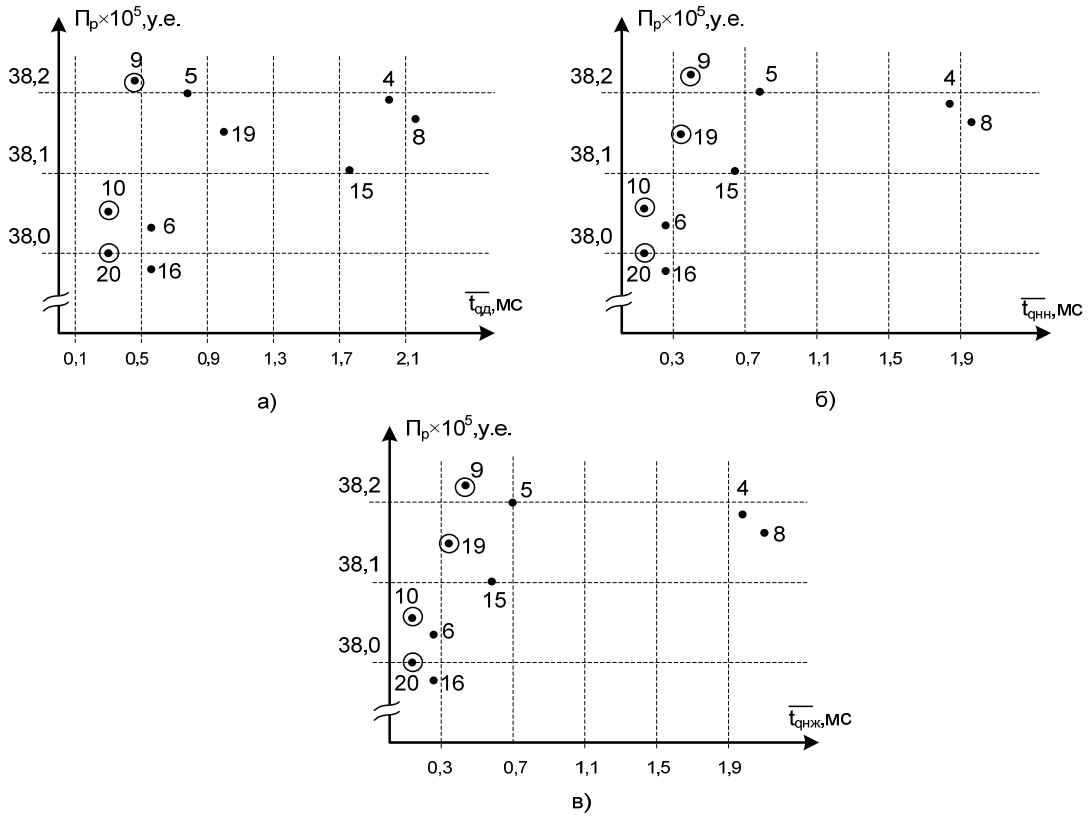


Рис. 1. Нахождение множеств Парето отдельно для каждого типа информации

Как видно из рисунков множества Парето для разных типов информации имеет вид: рис.1а) для данных: $\Omega_P^{д} = \{9, 10, 20\}$,рис.1б) для несжатой НИ: $\Omega_P^{нн} = \{9, 10, 19, 20\}$, рис.1в) для сжатой НИ: $\Omega_P^{нж} = \{9, 10, 19, 20\}$.

На втором этапе найдем окончательное решение о множестве вариантов построения сети, применив к полученным множествам Парето для данных, несжатой и сжатой НИ процедуру пересечения. Тогда в результате этой операции $\Omega_P^{д \cap нн \cap нж} = \Omega_P^{д} \bigcap \Omega_P^{нн} \bigcap \Omega_P^{нж}$ получим решение о выбранном множестве $\Omega_P^{д \cap нн \cap нж} = \{9, 10, 20\}$. Если же применим процедуру объединения полученных на первом этапе множеств $\Omega_P^{д \cup нн \cup нж} = \Omega_P^{д} \bigcup \Omega_P^{нн} \bigcup \Omega_P^{нж}$, то окончательное решение будет иметь вид $\Omega_P^{д \cup нн \cup нж} = \{9, 10, 19, 20\}$.

СПИСОК ЛИТЕРАТУРЫ

1. Доронин А. И. Бизнес-разведка. – 5-е изд., перераб. и доп. – М.: Ось-89, 2013. 704 с.
2. Татарникова Т. М. Защищенные корпоративные сети: задачи по защите информации. СПб: РГГМУ, 2012. 113 с.
3. Чугреев О. С., Верзун Н. А. Управление структурой локальных информационных сетей // Сборник трудов международной конференции ICI&I'97. – СПб., 1997. С.248–250.
4. Чугреев О. С., Верзун Н. А.Анализ пакетной передачи непрерывной информации со сжатием в локальных сетях с интеграцией служб. Сборник трудов международной конференции по информационным сетям и системам ISINAS-94. – СПб, 1994. С.165-168.
5. Верзун Н. А. Регулируемый доступ при передаче непрерывной информации со сжатием. 50-й НТК СПбГУТ. – СПб.,1997. С.144-145.

УДК 004.75

ОБМЕН И УДАЛЕННАЯ ОБРАБОТКА ИНФОРМАЦИИ В ДВУХУРОВНЕВОЙ АССОЦИАЦИИ СИСТЕМ МНОЖЕСТВЕННОГО ДОСТУПА

Верзун Наталья Аркадьевна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mail: dina_25@hotbox.ru.

Аннотация: Представлена математическая модель процессов передачи пользовательской и административной информации в двухуровневой ассоциации систем множественного доступа. Обмен информацией между пользователями и удаленная обработка моделируется многофазными СМО в дискретном времени.

Ключевые слова: *ассоциация систем множественного доступа; сеть обмена; серверная сеть; удаленная обработка информации; маркерный метод доступа.*

EXCHANGE AND REMOTE DATA PROCESSING TWO-TIER ASSOCIATION MULTIPLE ACCESS

Verzun Natalia,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: dina_25@hotbox.ru.

Abstract: Proposed a mathematical model of the processes the transfer of user information and administrative information in a two-tier association multiple-access systems. Exchange of information between users and remote processing simulated multiphase serving system in discrete time.

Keywords: *association multiple access; network exchange; server network; remote data processing; marker access method.*

Введение. Одной из актуальных проблем в современных системах связи является управление процессами в телекоммуникационных сетях. При этом используется автоматизация управления, в том числе административного, за счет конвергенции телекоммуникационных и компьютерных систем[1],[2]. Это приводит к введению в реализацию управления процессами обработки управляющей информации, а также технологиям множественного доступа[3],[4].

Рассматривается математическое моделирование процессов передачи пользовательской и административной информации в ассоциации систем множественного доступа[5].

1.Описание объекта моделирования. Физическая структура ассоциации систем множественного доступа представлена на рисунке1

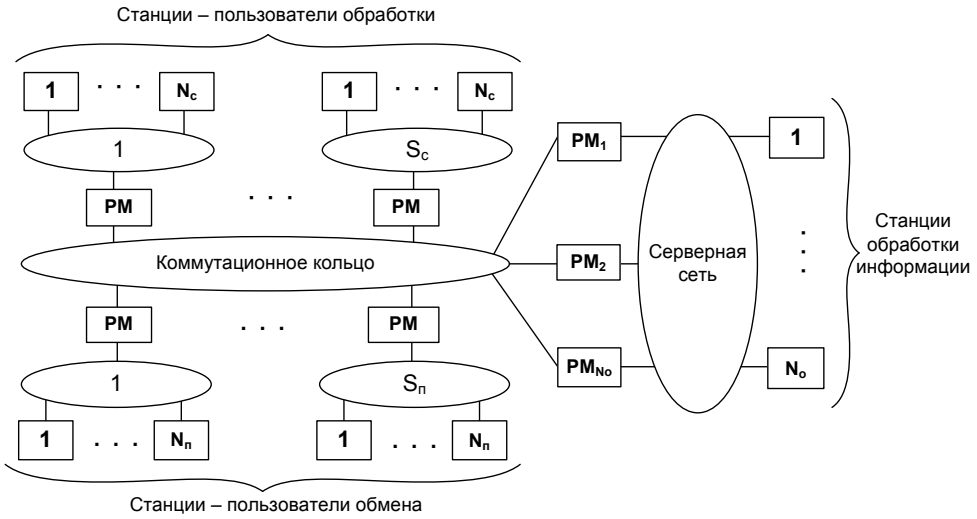


Рис. 1. Физическая структура ассоциации систем множественного доступа

Ассоциация имеет иерархическую структуру с двумя уровнями. Нижний уровень состоит из компонентов следующего типа: Sc сетей пользователей обработки, в каждой из которых предполагается Nсстанций пользователей обработки, Sп сетей пользователей обмена, каждая из которых включает в себя Nп станций пользователей обмена, а также серверной сети, состоящей из Nостанций обработки информации. Всесети нижнего уровня предполагаются кольцевой топологии.

Верхний по иерархии уровень – коммутационное кольцо(КК), в которое включаются посредством мостов сети нижнего уровня. Для каждой сети пользователей сервера и сети пользователей обмена предполагается одинраспределенный мост(РМ) подключения к КК. Для подключения серверной сети к КК предполагается количество мостов равное числу серверов(станций обработки информации) в серверной сети.

В ассоциации возможны следующие варианты передачи/обработки информации:

I–обмен информацией между пользователями внутри одной сети обмена

II–обмен информацией между пользователями различных сетей обмена

III– удаленная обработка запросов станций пользователей обработки станциями, входящими в состав серверной сети

Рассмотрим математическое моделирование трех вышеперечисленных процессов передачи/обработки информации для случая использования маркерного метода доступа к среде передачи во всех сетях ассоциации.Коммуникационные системы станций всех типов представляются СМО Мд/Gд/1.Предположим, что на входы станций пользователей обмена и пользователей обработки поступают потоки пакетов данных, описываемые распределением Бернулли с параметрами $q_{\text{ип}}$ и $q_{\text{ио}}$ соответственно на интервале T ($T = V_c^{-1}$, где V_c – скорость передачи в среде).Для станций пользователей обмена возможны 2 варианта обмена: между станциями одной сети обмена и между станциями разных сетей обмена. Введем параметр $\kappa_з$ – коэффициент замыкания, который показывает, какая доля передаваемого потока пакетов данных “остается” внутри сети обмена, соответственно $(1-\kappa_з)$ показывает долю информации, предназначенную для передачи пользователям обмена, относящимся к другим сетям. Тогда для Iи IIпроцесса обмена интенсивность входного потока будет соответственно иметь вид:

$$\lambda_{\text{ипI}} = \kappa_з \lambda_{\text{ип}},\ \lambda_{\text{ипII}} = (1-\kappa_з)\lambda_{\text{ип}},\quad \lambda_{\text{ип}} = q_{\text{ип}} \cdot T^{-1}, \tag{1}$$

где $\lambda_{\text{ип}}$ – общая интенсивность поступающего на станцию обмена потока пакетов.Предположим, что $\lambda_{\text{ипII}}$ “распределяется” равномерно между сетями обмена, таким образом, интенсивность входного потока со стороны КК(от РМ) в каждую сеть станций обмена будет иметь вид:

$$\lambda_{\text{ип3}} = \frac{S_{\text{п}} \lambda_{\text{ипII}}}{(S_{\text{п}} - 1)}, \tag{2}$$

где $S_{\text{п}}$ – число сетей пользователей обмена.

Для III-процесса интенсивность входного потока на станцию пользователя обработки

$$\lambda_{\text{ио}} = q_{\text{ио}} \cdot T^{-1} \tag{3}$$

2.Математическая модель процесса обмена информацией между станциями различных сетей обмена. Процесс обмена информацией между пользователями разных сетей обмена моделируется трехфазной СМО: на первой и второй фазе осуществляется передача информации от станции пользователя в сеть обмена и из сети в КК соответственно, а на третьей фазе предусмотрена передача информации из КК в другую сеть обмена. Математическая модель процесса обмена информацией между станциями различных сетей обмена – II-процесса можно представить с помощью выражения для z-преобразование ряда распределения (z-прр) времени задержки передачи пакета от станции одной подсети обмена станции другой подсети обмена $f_{q\text{пII}}(z)$

$$f_{q\text{пII}}(z) = f_{q\text{п}1}(z) f_{q\text{п}2}(z) f_{q\text{п}3}(z), \tag{4}$$

где $f_{q\text{п}1}(z)$ – *z*-прррвремени задержки передачи пакета от станции пользователя в сетьобмена (1 фаза), $f_{q\text{п}2}(z)$ – *z*-прррвремени задержки передачи пакета из сети обмена(от РМ) в КК (2 фаза), $f_{q\text{п}3}(z)$ –z-прр времени задержки передачи пакетаиз КК(от РМ)в сеть обмена (3 фаза); с учетом используемой модели $M^{\text{д}}/G^{\text{д}}/1$ выражения для $f_{q\text{п}1}(z)$, $f_{q\text{п}2}(z)$, $f_{q\text{п}3}(z)$ имеют следующий вид:

$$f_{qi}(z) = \frac{(1-\Theta_i)(1-z)\, g_i(z)}{1 - p_{\text{и}i}\, z - q_{\text{и}i}\, z\, g_i(z)},\ i = \overline{\text{п}1, \text{п}2, \text{п}3},\ q_{\text{ип}1} = \lambda_{\text{ип}} \cdot T,\ q_{\text{ип}2} = N_{\text{п}} \cdot \lambda_{\text{ипII}} \cdot T,\ q_{\text{ип}3} = \lambda_{\text{ип}3} \cdot T,$$
$$p_{\text{и}i} = 1 - q_{\text{и}i},\ \Theta_i = q_{\text{и}i}\, \overline{n_{si}},\ \overline{n_{si}} = (d/dz^{-1}) g_i(z)\big|_{z=1},\ \Theta_i < 1,\ i = \overline{\text{п}1, \text{п}2, \text{п}3}, \tag{5}$$

где $\Theta_i,\ i = \overline{\text{п}1, \text{п}2, \text{п}3}$ – вероятностизанятости буферов: станции обмена, РМ сети обмена, из которой идет передача и РМ сети обмена, в которую идет передача соответственно, интенсивности

$\lambda_{\text{ип}}, \lambda_{\text{ипII}}$ определяются из (1), а $\lambda_{\text{ип3}}$ из (2), $\overline{n_{si}}, i = \overline{\text{п1}, \text{п2}, \text{п3}}$ –длительность (в тактах системы) среднего интервала обслуживания на 1, 2 и 3 фазе соответственно, $g_i(z), i = \overline{\text{п1}, \text{п2}, \text{п3}}$ – z-прр интервала обслуживания 1, 2 и 3 фазы определяется (если предположить для всех фаз режим прямой передачи – без переспросов) следующим образом:

$$g_{\text{п1}}(z) = z^{-c_{\text{икп}}}(\overline{\Theta_{\text{п1}}} z^{-c_0} + \Theta_{\text{п1}} z^{-c_{\text{икп}}})^{N_{\text{п}}-1}(\overline{\Theta_{\text{п3}}} z^{-c_0} + \Theta_{\text{п3}} z^{-c_{\text{икп}}}),$$
$$g_{\text{п2}}(z) = z^{-c_{\text{икп}}}(\overline{\Theta_{\text{п2}}} z^{-c_0} + \Theta_{\text{п2}} z^{-c_{\text{икп}}})^{S_{\text{п}}-1}(\overline{\Theta_{\text{о2}}} z^{-c_0} + \Theta_{\text{о2}} z^{-c_{\text{икз}}})^{S_{\text{с}}}(\overline{\Theta_{\text{о4}}} z^{-c_0} + \Theta_{\text{о4}} z^{-c_{\text{икотв}}})^{N_{\text{о}}}, \quad (6)$$
$$g_{\text{п3}}(z) = z^{-c_{\text{икп}}}(\overline{\Theta_{\text{п1}}} z^{-c_0} + \Theta_{\text{п1}} z^{-c_{\text{икп}}})^{N_{\text{п}}}, \overline{\Theta_j} = 1 - \Theta_j, \Theta_j < 1, j = \overline{\text{п1}, \text{п2}, \text{п3}, \text{о2}, \text{о4}},$$

где $c_{\text{икп}}$ – длительность временного окна доступа станции обмена или РМ(сети обмена), в случае если у станции или РМ(сети обмена) есть пакет для передачи (с вероятностью $\Theta_i, i = \overline{\text{п1}, \text{п2}, \text{п3}}$), $c_{\text{икз}}$ – длительность временного окна доступа РМ (сети пользователей обработки), в случае если у РМ (сети обработки) есть пакет-запрос на обработку для передачи (с вероятностью Θ_{o2}), $c_{\text{икотв}}$ – длительность временного окна доступа РМ (серверной сети), в случае если у РМ (серверной сети) есть пакет-запрос на обработку для передачи (с вероятностью Θ_{o4}), c_0 – длительность временного окна передачи маркера станцией или РМ, в случае если у станции или РМ нет пакета для передачи (с вероятностью $\overline{\Theta_j}, j = \overline{\text{п1}, \text{п2}, \text{п3}, \text{о2}, \text{о4}}$), выражения для расчета Θ_{o2} и Θ_{o4} см. ниже в п.4. выражение (9).Расчет длительности временных окон проводится с учетом используемого режима передачи, например, так как представлено в [4],[6].

3.Математическая модель процесса обмена информацией внутри одной сети обмена. Процесс передачи информации внутри одной сети обмена(I процесс) можно представить однофазной СМО с помощью следующих выражений: z-прр времени задержки при передаче пакета внутри сети обмена:

$$f_{q\text{пI}}(z) = \frac{(1-\Theta_{\text{п1}})(1-z)\, g_{\text{п1}}(z)}{1 - p_{\text{ип}}\, z - q_{\text{ип}}\, z\, g_{\text{п1}}(z)}; \Theta_{\text{п1}} < 1, \quad (7)$$

где $\Theta_{\text{п1}}$ – вероятность того, что у станции обмена в буфере есть пакет для передачиопределяется из (5), $g_{\text{пI}}(z)$ – z-прр интервала обслуживания определяется из(6).

4.Математическая модель процесса удаленной обработки информации. Требования на обработку информации генерируются станциями пользователей серверов [7]. Процесс удаленной обработки информации моделируется пятифазной СМО. На первойфазепроисходит передача запроса на обработку от станции в сеть пользователей обработки, на второй – в КК, на третьей осуществляется передача запроса станции обработки, обработка, формирование и передача пакета-ответана запрос, четвертая фаза – передача ответа в КК, пятая – передача ответа из КК в сеть пользователей обработки.Математическая модель процесса удаленной обработки информации – III-процесса можно представить с помощью выражения для z-прр времени задержки при удаленной обработке информации в ассоциации $f_{q\text{оIII}}(z)$

$$f_{q\text{оIII}}(z) = f_{q\text{о1}}(z) f_{q\text{о2}}(z) f_{q\text{о3}}(z) f_{q\text{о4}}(z) f_{q\text{о5}}(z), \quad (8)$$

где $f_{q\text{о1}}(z)$ – z-прр времени задержки передачи запроса на обработку от станции пользователя обработкив сеть пользователей обработки(1 фаза), $f_{q\text{о2}}(z)$ – z-прр времени задержки передачи пакета-запроса из сети пользователей обработки (от РМ) в КК (2 фаза), $f_{q\text{о3}}(z)$ – z-прр времени задержки передачи запроса станции обработки, обработка, формирование и передача пакета-ответа на запрос(3 фаза); $f_{q\text{о4}}(z)$ – z-прр времени задержки передачи пакета-ответа из серверной сети (от РМ) в КК (4 фаза), $f_{q\text{о5}}(z)$ – z-прр времени задержки передачи пакета-ответа из КК(от РМ) в сетьпользователей обработки (5 фаза);с учетом используемой модели Мд/Gд/1 выражения для $f_{q\text{о1}}(z)$, $f_{q\text{о2}}(z)$, $f_{q\text{о3}}(z)$, $f_{q\text{о4}}(z)$, $f_{q\text{о5}}(z)$ имеют следующий вид:

$$f_{qj}(z)=\frac{(1-\Theta_j)(1-z)\,g_j(z)}{1-p_{ij}\,z-q_{ij}\,z\,g_j(z)},\ \Theta_j=q_{ij}\overline{n_{sj}},\ \overline{n_{sj}}=(d/dz^{-1})g_j(z)\big|_{z=1},\ \Theta_j<1,$$

$$p_{ij}=1-q_{ij},\ j=\overline{\text{о1},\text{о2},\text{о3},\text{о4},\text{о5}},\ q_{\text{ио1}}=\lambda_{\text{ио}}\cdot T,\ q_{\text{ио2}}=q_{\text{ио5}}=N_{\text{с}}\cdot\lambda_{\text{ио}}\cdot T,$$

$$q_{\text{ио3}}=q_{\text{ио4}}=\frac{N_{\text{с}}\cdot\lambda_{\text{ио}}\cdot S_{\text{с}}}{N_{\text{о}}}\cdot T, \qquad (9)$$

где $\Theta_j,\ j=\overline{\text{о1},\text{о2},\text{о3},\text{о4},\text{о5}}$ – вероятности занятости буферов: Θ_{o1} станции пользователя обработки, Θ_{o2} –РМ сети пользователей обработки, из которой идет передача запроса на обработку, $\Theta_{\text{о3}}$ –РМ серверной сети (в направлении к сети), $\Theta_{\text{о4}}$ –РМ серверной сети (в направлении к КК) и Θ_{o5} –РМ сети пользователей обработки, в которую идет передача ответа на запрос-обработку, интенсивности $\lambda_{\text{ио}}$ определяется из (3), $\overline{n_{si}},\ i=\overline{\text{п1},\text{п2},\text{п3}}$ – длительность (в тактах системы) среднего интервала обслуживания на 1, 2, 3, 4 и 5 фазе соответственно, $g_j(z),\ j=\overline{\text{о1},\text{о2},\text{о3},\text{о4},\text{о5}}$ – z-прр интервала обслуживания 1, 2, 3, 4 и 5 фазы определяется (если предположить для всех фаз режим прямой передачи – без переспросов) следующим образом:

$$g_{\text{о1}}(z)=z^{-c_{\text{икз}}}(\overline{\Theta_{\text{о1}}}z^{-c_0}+\Theta_{\text{о1}}z^{-c_{\text{икз}}})^{N_{\text{с}}-1}(\overline{\Theta_{\text{о5}}}z^{-c_0}+\Theta_{\text{о5}}z^{-c_{\text{икотв}}}),$$

$$g_{\text{о2}}(z)=z^{-c_{\text{икз}}}(\overline{\Theta_{\text{о2}}}z^{-c_0}+\Theta_{\text{о2}}z^{-c_{\text{икз}}})^{S_{\text{с}}-1}(\overline{\Theta_{\text{п2}}}z^{-c_0}+\Theta_{\text{п2}}z^{-c_{\text{икп}}})^{S_{\text{п}}}(\overline{\Theta_{\text{о4}}}z^{-c_0}+\Theta_{\text{о4}}z^{-c_{\text{икотв}}})^{N_{\text{о}}},$$

$$g_{\text{о3}}(z)=z^{-c_{\text{обр}}}(\overline{\Theta_{\text{о3}}}z^{-c_0}+\Theta_{\text{о3}}z^{-c_{\text{обр}}})^{N_{\text{о}}-1},$$

$$g_{\text{о4}}(z)=z^{-c_{\text{икотв}}}(\overline{\Theta_{\text{о4}}}z^{-c_0}+\Theta_{\text{о4}}z^{-c_{\text{икотв}}})^{N_{\text{о}}}(\overline{\Theta_{\text{п2}}}z^{-c_0}+\Theta_{\text{п2}}z^{-c_{\text{икп}}})^{S_{\text{п}}}(\overline{\Theta_{\text{о4}}}z^{-c_0}+\Theta_{\text{о4}}z^{-c_{\text{икотв}}})^{N_{\text{о}}}, \qquad (10)$$

$$g_{\text{о5}}(z)=z^{-c_{\text{икотв}}}(\overline{\Theta_{\text{о1}}}z^{-c_0}+\Theta_{\text{о1}}z^{-c_{\text{икз}}})^{N_{\text{с}}},$$

$$\overline{\Theta_j}=1-\Theta_j,\ \Theta_j<1,\ j=\overline{\text{п1},\text{п2},\text{п3},\text{п4},\text{п5},\text{о2},\text{о4}},$$

где $c_{\text{икз}}$ – длительность временного окна доступа станции пользователя обработки или РМ (сети обработки), в случае если у станции или РМ (сети обработки) есть пакет-запрос на обработку для передачи (с вероятностями $\Theta_j,\ j=\overline{\text{о1},\text{о2}}$), $c_{\text{икотв}}$ – длительность временного окна доступа РМ серверной сети и РМ сети пользователей обработки, в случае если у РМ есть пакет-ответ для передачи (с вероятностями $\Theta_j,\ j=\overline{\text{о4},\text{о5}}$). $c_{\text{обр}}$ – длительность временного окна обработки пользовательского запроса в серверной сети, в случае если у РМ есть пакет-запрос на обработку (с вероятностью $\Theta_{\text{о3}}$), c_0 – длительность временного окна передачи маркера станцией или РМ, в случае если у станции или РМ нет пакета для передачи/обработки (с вероятностью $\overline{\Theta_j},\ j=\overline{\text{п1},\text{п2},\text{п3},\text{п4},\text{п5},\text{о2},\text{о4}}$), Расчет длительности временных окон передачи можно провести, например, так как представлено в [4],[6]. Расчет длительности временного окна обработки зависит от используемого алгоритма удаленной обработки информации. В выражениях для математической модели III-процесса (9),(10) предусматривается режим обработки с удержанием канала, подобный метод и расчет длительности $c_{\text{обр}}$ для данного случая рассматривался,например, в [8].

Заключение. Представленная математическая модель ассоциации неоднородных систем может служить основой для разработки методов расчета вероятностно-временных характеристик процессов передачи информации: внутри одной подсети обмена – выражения (5, 6, 7), между станциями различных подсетей обмена – выражения (4, 5, 6); процесса удаленной обработки информации – выражения (8,9,10), которые позволят проводить численный анализ процессов передачи и удаленной обработки в ассоциации неоднородных систем множественного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю. Ф., Колбанёв М. О. Технология инфокоммуникации. Курск: Науком, 2011.260 с.
2. Советов Б. Я., Цехановский В. В., Чертовской В. Д. Интеллектуальные системы и технологии. М.: Академия, 2013. 320 с.
3. Чугреев О. С., Верзун Н. А., Клевакичев С. И. Множественный доступ к доставке и обработке неоднородной информации. VI Международный форум по информатизации ISINAS-2000. – СПб., 2000. С.345-357.
4. Верзун Н. А. Множественный доступ в информационных системах. Учебное пособие. СПб.: СПбГУТ, 2007. 92 с.

5. Верзун Н. А.Математическая модель и методы расчета характеристик ассоциации неоднородных локальных систем с детерминированным методом доступа. 57-й НТК СПбГУТ. – СПб., 2005. С.129.
6. Чугреев О. С., Верзун Н. А. Модель интегрированной информационной системы синхронного временного доступа. Международный семинар "Информационные сети, системы и технологии". Ч.1: Телекоммуникационные сети и системы. Материалы семинара. – Ярославль, 1997.С.64-68.
7. *Колбанёв М.О., Татарникова Т.М., ВоробьёвА.И.*Модель обработки клиентских запросов//Телекоммуникации. 2013 №9. С. 42-48.
8. Верзун Н. А. Моделирование и расчет характеристик неоднородной информационной системы с обработкой информации в режиме удержания канала. 55-й НТКСПбГУТ. – СПб.,2003. С.24.

УДК 004.89, 004.622, 004.056.2

МОДЕЛЬ АВТОРА И ТЕКСТА В РЕШЕНИИ ЗАДАЧИ ИДЕНТИФИКАЦИИ АВТОРА АНОНИМНЫХ СООБЩЕНИЙ В СЕТИ ИНТЕРНЕТ

Воробьева Алиса Андреевна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики «НИУ ИТМО»,
Россия, Санкт-Петербург, Кронверский пр., 49,
e-mail: alice_w@mail.ru.

Аннотация: Задача идентификации анонимных пользователей Интернет порталов становится все более актуальной научной задачей, это обусловлено ростом числа интернет пользователей, в том числе анонимных, ростом числа случаев совершения противоправных действий (например, анонимных угроз и экстремистских высказываний) и несовершенством существующих подходов и алгоритмов идентификации анонимных пользователей.
В контексте работы под идентификацией автора и пользователя понимается распознавание анонимного пользователя в Интернете. Распознавание производится путем соотнесения набора характеристик анонимного пользователя с характеристиками, собранными ранее и уже имеющимися в базе данных. К характеристикам пользователя относится ряд лингвистических характеристик текста – стиль письменной речи автора сообщения. В статье рассматривается возможность идентификации пользователей по различным наборам таких характеристик. Анализируется возможность применения различных методов классификации (метод опорных векторов, нейросети, логическая регрессия) для решения задачи по идентификации анонимных пользователей.
Проведенные эксперименты показали, что использование метода опорных векторов позволяет повысить точность идентификации анонимного пользователя Интернет портала.

Ключевые слова: *идентификация анонимных пользователей; атрибуция автора; авторство сообщений; информационная безопасность; компьютерная криминалистика.*

THE AUTHOR AND TEXT MODEL IN THE SOLUTION OF ANONYMOUS MESSAGE AUTHOR IDENTIFICATION TASK IN INTERNET NETWORK

Vorobeva Alisa Andreevna,
St. Petersburg State University of Information Technologies, Mechanics and Optics «ITMO» Russia,
Russia, St-Petersburg, Kronversky ave., 49,
e-mail: alice_w@mail.ru

Annotation: In recent years, the task of identifying anonymous web users became important research task. The number of users dramatically increases, as a frequency of using Internet for criminal purposes (such as anonymous threats and extremist statements). Existing approaches and algorithms for identifying author of short anonymous message on Russian language are not enough efficient.
In the context of the work author identification means recognizing anonymous user on the Internet. Identification is performed by correlating the set of features of anonymous user with the previously collected features, stored in the database. Feature set of user consists of writing-style features of the text (for short texts on Russian language). In this work the discriminating power of several feature sets and of three classification methods (Support Vector Machines, neural networks, logistic regression) are compared. The experimental results showed that the usage of Support Vector Machines classification method improves the accuracy of identification of an anonymous user of the Internet.

Key words: *anonymous user identification; authorship of text message; author attribution; information security, computer forensics.*

Введение. Актуальность исследования возможности идентификации автора анонимных сообщений, размещенных в сети Интернет, обусловлена следующим:

– ростом количества преступлений и противозаконных действий, совершенных при помощи Интернет средств Интернет переписка, как подготовка к совершению реального преступления,

анонимные злонамеренные сообщения, анонимные сообщения экстремистского характера, создание сообщений с заведомо ложным авторством, с целью компрометации «честного имени») [1], [2], [3] [4];

– постоянным ростом числа Интернет пользователей, в том числе анонимных;

– несовершенством существующих способов идентификации анонимных пользователей [5];

– несовершенством существующих способов атрибуции автора коротких сообщений на русском языке.

На сегодняшний день существует несколько типов подходов к идентификации пользователя Интернет-порталов [6]:

1. На основании характеристик программного и аппаратного окружения пользователя.
2. На основании поведенческих характеристик пользователя на портале.
3. На основании стилистических характеристик письменной речи пользователя.

Первые два типа обладают следующими общими недостатками или ограничениями:

– необходимо использование дополнительных серверных компонент или дополнений к веб-браузеру,

– они не применимы для постинцедентного анализа.

Все существующие способы идентификации на основании стилистических характеристик письменной речи пользователя можно разбить на две группы: разработанные для коротких текстов на иностранных языках и разработанные для текстов литературных произведений. Их ограничения приведены ниже:

1. Они предназначены для идентификации автора текста на иностранном языке и вполне логично, что они не применимы для русских кириллических текстов, в силу особенностей каждого языка.

2. Они предназначены для идентификации автора литературного произведения, то есть для текста прошедшего предварительную корректировку и рецензирование. Но основным ограничением является то, что данные способы предназначены для работы с текстами достаточно больших объемов, более 20 000 символов.

Подводя итог вышесказанному, можно смело сказать, что на сегодняшний день не разработаны методы идентификации, позволяющие получить достаточную точность в условиях накладываемых ограничений. Существует необходимость проведения постинцидентного анализа без использования дополнительных серверных компонент или дополнений к веб-браузеру.

Цель работы. Целью работы является повышение точности идентификации или атрибуции автора анонимного сообщения, с использованием лингвистических или стилистических характеристик текста. В качестве идентификатора автора предлагается использовать уникальную комбинацию лингвистических признаков.

Модель автора и текста. В общем случае, задача атрибуции автора сообщений интернет порталов сводится к решению задачи многоклассовой классификации. Имеется множество пользователей $U = \{u1,...,uk\}$ и множество текстов $T = \{t1,...tn\}$. Некоторое подмножество текстов $T' = \{t1,...,tm\} \subseteq T$ атрибутируется определенному пользователю, т.е. существует множество пар «текст-пользователь» $Ttr = (ti, ui)_{i=1}^{m}$. Необходимо установить, кому из множества U действительно принадлежат остальные тексты $T' = \{tm+1,...,tn\} \subseteq T$, требуется построить алгоритм а: $T \to U$, способный классифицировать произвольный текст из исходного множества – $t_i \in T$.

В ходе предыдущих исследований [7], [8] были отобраны наиболее эффективные методы классификации. Были выбраны следующие методы классификации: метод опорных векторов, нейронные сети. Однако, в ходе исследования было принято решение исключить нейронные сети, в силу того, что с ростом количества признаков время работы существенно увеличивается.

В данной работе, текст рассматривается, как вектор в пространстве признаковых описаний R^n, где n – это количество частотных характеристик текста, признаков, являющееся одинаковым для всех текстов. Полагая, что пользователь обладает некоторыми свойственными ему стилистическими характеристиками, можно сопоставить ему, как конкретному физическому лицу, определенные характеристики текста на естественном языке. То есть можно представить текст в виде вектора длиной n, где n – число выявленных характеристик.

Существует достаточно большое количество возможных характеристик текста, служащих признаками для идентификации автора. Характеристики текст могут быть сгруппированы по их типу: лексические уровня символов (Fls), лексические уровня слов (Flw), синтаксические (Fs), структурные (Fst).

$$Fls - (fls1,\ fls2,...,fls1-k);$$

$$Flw = (flw1,\ flw2,...,\ flwk - l);$$
$$Fs = (flw1,\ flw2,...,\ flwk - m);$$
$$Fst = (flw1,\ flw2,...,\ flwm - n).$$

Таким образом, текст представляется в виде:

$$T = F = (Fls, Flw, Fs, Fst) = (f1, f2,..., fn).$$

Так как текст обладает характеристиками, свойственными для его автора, тогда представляется возможным определить автора u_j как кортеж, координатам которого сопоставляется множество характеристик, обусловленных стилистическими особенностями его письменной речи, fn. Пользователь представляется, как:

$$u_j = t_j = fj = \{ fls_j, fwl_j, fs_j, fst_j \},$$
$$u_j \in U,\ t_j \in T,\ f_j \in F,\ fls_j \in Fls,\ fwl_j \in Flw,\ fs_j \in Fs,\ fst_j \in Fst,$$

где f_j – совокупные характеристики текста, F – множество возможных значений совокупных характеристик текста, fls_j – лексические характеристики текста t_j уровня символов, fwl_j – лексические характеристики текста t_j уровня слов, fs_i – синтаксические характеристики текста t_j, fst_j – структурные характеристики текста t_j, Fls – множество возможных значений лексических характеристик текста уровня символов, Flw – множество возможных значений лексических характеристик текста уровня слов, Fs – множество возможных значений синтаксических характеристик текста, Fst – множество возможных значений структурных характеристик текста. Описание конкретных характеристик текста приводится в работах [7] и [8].

Метод идентификации. В этой работе для решения задачи идентификации предлагается использовать подход, основанный на методе опорных векторов(SVM – Support Vector Machine), разработанный В.Н. Вапником. Этот подход по многим показателям, таким как время построения модели, время работы классификатора, точность классификации показал себя более эффективным, по сравнению с другими анализируемыми методами классификации, что было доказано в предыдущих исследованиях [7] и [8].

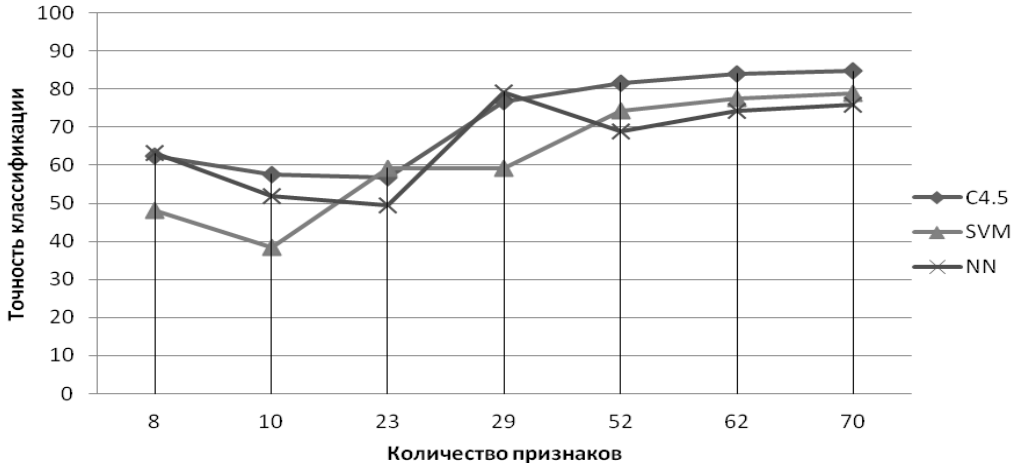


Рис. 1. Время работы классификатора

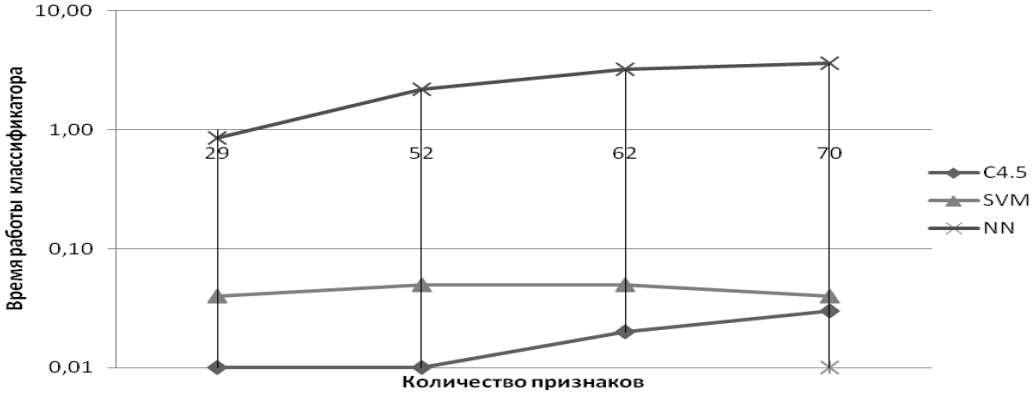


Рис. 2. Точность различных методов классификации

Метод опорных векторов особенно полезен в случае большого числа классификационных признаков. Он обладает высокой точностью классификации, однако при работе с большими объемами данных, время обучения очень велико и увеличивается пропорционально квадрату числа обучающих примеров. Время обучения машины опорных векторов может быть существенно снижено при распараллеливании алгоритмов SVM. Предлагается использовать имплементацию алгоритма SVM, позволяющую производить обучение машины опорных векторов параллельно, на базе алгоритма минимальной последовательной оптимизации (SMO – sequential minimal optimization) с применением методов кластеризации. Таким образом, для решения задачи идентификации автора анонимного сообщения был выбран алгоритм SVM/SMO.

В оригинале метод опорных векторов представляет собой линейный классификатор, способный решать только линейно разделимые задачи, к которым не относится задача идентификации (классификации) автора. Однако, применяя нелинейную функцию ядра классификатора, существует возможность отразить исходные данные – вектор текста в пространство большей размерности. Что позволит построить такую оптимальную разделяющую гиперплоскость, которая сможет произвести разделение по классам.

Наш линейный классификатор в пространстве R^n может быть представлен в виде функции $a^t x + b, cn + 1(\approx n_1 * n_2 + 1)$ параметрами $(b, a_i, i = 1,...,n)$. Расположение характеристик в векторной модели не влияет на то, насколько хорошо будет работать данная модель. В качестве ядра классификатора используется полином степени k, параметр регуляризации $C = 1$, допустимый уровень ошибки – 0,00001.

Результаты и выводы

Предлагаемый метод классификации – метод опорных векторов, позволяет получить наиболее высокие показатели точности классификации при решении задачи идентификации автора анонимного сообщений.

При проведении сравнения по времени работы классификатора, метод SVM также является лидером. Он особенно полезен в случае большого числа классификационных признаков, и увеличение числа классификационных признаков существенно не влияет на время работы классификатора.

Предлагаемый подход к идентификации автора анонимных сообщений эффективно работает и показывает стабильно высокие результаты в тех случаях, когда другие способы идентификации не возможны. Например, в случае, когда инцидент уже произошел, но на портале не велся учет характеристик пользователя. Также возможно производить идентификацию пользователей, в случае, если отсутствует возможность внедрения дополнительных компонентов учета и регистрации на сервер Интернет портала. Этот подход работает в достаточно жестко ограниченных условия: крайняя краткость сообщений пользователей.

В отличие от существующих подходов к идентификации анонимных пользователей, предлагаемый подход не требует внедрения на сервера Интернет порталов или установки в качестве дополнения к веб-браузеру, имеет функционал для анализа сообщений, написанных на русском языке.

Точность идентификации автора анонимных сообщений на русском языке является достаточно высокой и сопоставима с точностью, достигаемой исследователями для других языков.

СПИСОК ЛИТЕРАТУРЫ

1. O de Vel, A. Anderson, M. Corney, G Mohay. Mining e-mail content for author identification forensics. – [б. м.]: SIGMOD Rec., 2001, T. 30(4), p. 55–64.
2. Abbasi A., Chen H.: Applying Authorship Analysis to Extremist-group Web Forum Messages. IEEE Intelligent Systems, 20(5), 67–75 (2005).
3. Zheng R., Li J., Chen H., Huang Z. Authorship analysis in cybercrime investigation, In ISI'03: Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics, – [б. м.]: Berlin, Heidelberg, Springer-Verlag, 2003. – T. pages 59–73.
4. Stamatatos E. A Survey of Modern Authorship Attribution Methods Journal of the American Society for Information Science and Technology, 60(3), pp. 538–556, 2009, Wiley.
5. Stamatatos E. On the Robustness of Authorship Attribution Based on Character n-gram Features, Journal of Law and Policy, 21(2), pp. 421–439, Brooklyn Law School, 2013.
6. Ivбncsy R., Juhбsz S. Analysis of Web User Identification Methods, International Journal of Computer Science; 2007, Vol. 2 Issue 3, p 212.
7. Воробьева А.А. Анализ возможности применения различных лингвистических характеристик и алгоритмов классификации для идентификации автора // Информация и космос. – Санкт-Петербург, 2013. – Вып. 5. – ISSN 2072-9804.
8. Воробьева А.А., Гвоздев А.В. Идентификация анонимных пользователей Интернет порталов на основании технических и лингвистических характеристик пользователя // Научно-технический вестник информационных технологий, механики и оптики. – Санкт-Петербург, 2014. – Вып. 1.– ISSN 2226–1494.

УДК 004.056.5

ДИСТАНЦИОННАЯ РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И ДОКУМЕНТОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Горелик Самуил Лейбович, Ляпер Виталий Сергеевич,
Санкт-Петербургскийнаучно-исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, д.49,
e-mails: samgor46@gmail.com, vitaly@lyaper.com.

Аннотация: В настоящей статье рассматривается процедура электронной регистрации, используемая при предоставлении современных инфокоммуникационных услуг, основной акцент делается на возможность в результате регистрации связать профиль пользователя услуги и личность пользователя. Для решения этой задачи разработана процедура регистрации общегражданского паспорта в составе профиля электронной услуги. Описывается набор неободимых мер, чтобы обеспечить достоверность такой регистрации и снизить риски для поставщика услуг.

Ключевые слова: *информационная безопасность; электронные услуги*.

REMOTE REGISTRATION OF USERS AND DOCUMENTS IN TELECOMMUNICATION SYSTEMS

Gorelik Samuil, Lyaper Vitaly,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St.Petersburg, 49 Kronverksky Ave,
e-mails: samgor46@gmail.com, vitaly@lyaper.com.

Abstract: This article examines the electronic registration procedure used in the provision of modern information and communication services, the main focus is on the ability to link to registration of the user profile service and the user's identity. Tosolvethisproblem a registration procedure of the passport as part of the profile of e-services is proposed. Describes a set of necessary measures to ensure the validity of such registration and reduce the risk fortheserviceprovider.

Keywords: *information security; e-services*

Введение

Стремление к сокращению издержек со стороны коммерческих организаций приводит к тому, что все больше из них, традиционно предпочитавших предоставлять услуги через сеть клиентских офисов, переходят на полностью дистанционные схемы предоставления услуг, главным образом, через Интернет.

Ряд современных услуг, предоставляемых в электронной форме, требует обязательной идентификации пользователя:

- банковское обслуживание;
- услуги налогового агента;
- заключение договоров через Интернет;
- переводы и платежи.

Единственным юридически значимым способом идентификации в настоящий момент является идентификация по общегражданскому паспорту Российской Федерации. Данный способ является безальтернативным до тех пор, пока не будут разработаны и законодательно подкреплены электронные удостоверения личности, например на базе универсальной электронной карты [1].

Паспорт гражданина РФ и его подлинность.

Паспорт гражданина Российской Федерации содержит несколько степеней защиты, многие из которых возможно проверить только при полноценном, всестороннем визуальном осмотре паспорта:

На Рис. 1 представлен разворот страниц 2 и 3 в видимом свете. На странице 2 бесцветной краской люминисцирующей в ультрафиолетовом излучении зеленым цвеетом нанесено слово «ПАСПОРТ» расположенное посередине. Страница 3 покрыта ламинирующей пленкой с нанесенными на неё линиями и узорами красного цвета, а также невидимой в обычных условиях и люминисцирующей под воздействием ультрафиолетового излучения многократно повторяющейся надписью «МВД РОССИИ». На странице также присутствует слово «РОССИЯ», нанесенное бесцветной краской, люминисцирующей зеленым цветом под воздействием ультрафиолетового излучения. Текстовые линейки на паспорте выполнены микрошрифтом с высотой букв 250 мкм с многократно повторяющимися словами:

1. «паспорт»
2. «дата»
3. «подразделение»

4. «код»
5. «подпись»
6. «фамилия»
7. «имя»
8. «отчество»
9. «пол»
10. «дата»
11. «паспорт»

Рис. 1. Паспорт гражданина РФ и его степени защиты

Также с 2011 года для ламинации используется новая плёнка, которую труднее удалить, на ней появился вензель с надписью «РФ», и со специальной голограммой. Кроме того в паспортах нового образца, выдаваемых с 1 июля 2011 года в России под фотографией появилось специальное поле с основной информацией о владельце паспорта.

Однако, подделка и подлог паспортов происходит повсеместно и непрерывно, основные способы подделки следующие:

– отслаивание ламината, замена имеющейся фотокарточки на новую фотокарточку и повторное ламинирование;

– вырезание фотокарточки и наклеивание на ее место новой с новым ламинатом;

– наклеивание на третью страницу паспорта (поверх ламината, фотокарточки и установочных данных) листа бумаги с имитированными реквизитами, фотокарточки и ламинирование новым ламинатом;

– удаление ламината, фотокарточки и поверхностного слоя бумаги с установочными данными, нанесение на бумагу имитированных изображений бланка, фотокарточки, установочных данных и ламинирование новым ламинатом;

– "расшивка" паспорта, удаление имеющегося листа и "вшивка" нового листа с имитированными реквизитами бланка, установочными данными, фотокарточкой и ламинатом.

Как можем видеть, проверить достоверность паспорта можно с большой долей вероятности только при полноценном визуальном осмотре, который невозможен при электронной регистрации этого документа. Следовательно, для усиления электронной регистрации паспорта и придания ей статуса аналогичного регистрации при личном присутствии, необходимо принимать специальные меры технического характера в процессе регистрации документа.

Электронная регистрация паспорта.

Процедура регистрации пользователя в системе электронных коммуникаций является одним из важнейших компонентов, от структуры которого и качетсва интерфейсов зависит “usability” системы.

В настоящее время в большинстве приложений (в том числе, в банковских и государственных услугах) обязательна первичная (полная) регистрация пользователя, во время которой производится его аутентификация на основе предъявляемого документа и привязка выдаваемого идентификатора к его личности [2]. В любом случае юридическая значимость в полном объеме может быть достигнута только после реализации указанной процедуры первичной регистрации. Однако, в практических применениях возможны подходы, использующие процедуру предварительной регистрации [2], [4], [5], в которой до момента необходимости совершения каких-либо взаимодействий, требующих

юридической ответственности участников, допускается привязка пользователя к идентификатору без процедуры его аутентификации. Полная регистрация производится только тогда, когда пользователь начинает использовать услуги, требующие аутентификации. Такой подход существенно повышает привлекательность и доступность ряда электронных услуг.

В настоящей статье рассматривается полная процедура регистрации, которая при необходимости может быть разбита на предварительный и основной этапы для повышения эргономичности. Ключевая же задача процедуры регистрации – создание связи между электронным идентификатором пользователя и его паспортом.

В случае предоставления заведомо поддельного или подложноного паспорта в процессе регистрации могут возникнуть риски, в т.ч. финансового характера, для организации, предоставляющей услугу. Недостатки электронных процедур регистрации с привязкой к личности могут быть использованы злоумышленниками с целью осуществления разного рода мошенничества.

Для снижения этих рисков и повышения достоверности при регистрации общегражданского паспорта была разработана процедура электронной регистрации для инфокоммуникационных услуг, позволяющая, помимо стандартной схемы создания профиля пользователя электронной услуги, привязать его к личности пользователя. Таким образом, в результате такой процедуры для электронной услуги создается взаимнооднозначная связь между электронным идентификатором пользователя, созданным в процессе регистрации, и его общегражданским паспортом.

В рамках разработанной процедуры регистрации общегражданского паспорта производится:

– сохранение в системе персональных данных пользователя: ФИО, паспортные данные, информация о регистрации, военной обязанности, семейном положении;

– сохранение отсканированных изображений страниц паспорта пользователя;

– идентификация гражданина по его паспорту уполномоченным оператором;

– дополнительные проверки полученного данных о паспорте гражданина РФ, через сторонние организации (например банки);

– регистрация помимо паспорта ещё одного документа (например водительского удостоверения), чтобы уменьшить вероятность предоставления недостоверных данных.

Разработанная процедура является дополнением к обычной процедуре регистрации для электронной услуги и может быть легко встроены в любые уже реализованные механизмы регистрации.

Для регистрации паспорта в системе дополнительно потребуется установить видеосвязь с уполномоченным оператором, посредством веб-камеры, видеокамеры или специализированного терминала, поддерживающего возможность видеосвязи с уполномоченным оператором, а также сканирующее устройство, позволяющее оператору получить отсканированные изображения паспорта, регистрирующегося лица. Взаимодействие при регистрации паспорта происходит следующим образом (показано на рис. 2).

Пошаговое описание процесса регистрации паспорта:

1. Пользователь заходит на сайт системы, где производится регистрация, либо входит в соответствующее меню специализированного терминала для регистрации в системе;
2. Пользователь посылает запрос на регистрацию паспорта в системе, сам паспорт прикладывается к сканирующему устройству разворотом 2-й и 3-й страниц, одновременно пользователь вводит номер своего мобильного телефона, который будет использован в дальнейшем как его идентификатор в комбинации с паролем, адрес электронной почты и выбирает псевдоним;
3. Устанавливается связь между устройством, с помощью которого выполняется регистрация, и уполномоченным оператором;
4. Уполномоченный оператор получает отсканированное изображение страниц паспорта лица, выполняющего регистрацию, одновременно он видит видеоизображение с места регистрации;
5. Оператор визуально производит сверку полученного изображения паспорта и регистрируемого лица, в случае успешной сверки подтверждает регистрацию паспорта. Дополнительно, если сканирующее устройство это позволяет можно получить изображение паспорта в ультрафиолетовом свете, что позволит проверить некоторые из способов защиты паспорта от подделки;
6. Пользователь подтверждает свой идентификатор – мобильный телефон – путем звонка на специальный номер или ввода одноразового пароля, полученного на телефон по SMS.
7. После подтверждения идентификатора пользователю, для проверки действительности его паспортных данных может быть предложена процедура верификации, через третью уполномоченную организацию, например банк. В этом случае пользователь должен предоставить номер своего банковского счета, на который ему будет переведена случайная сумма, а пользователь должен будет ввести эту сумму в систему. Узнать значение такой суммы пользователь сможет только получив доступ к своему счету, пройдя процедуру идентификации в банке, где его паспортные данные уже проверены, тем самым он подтвердит корректность предоставленной информации.

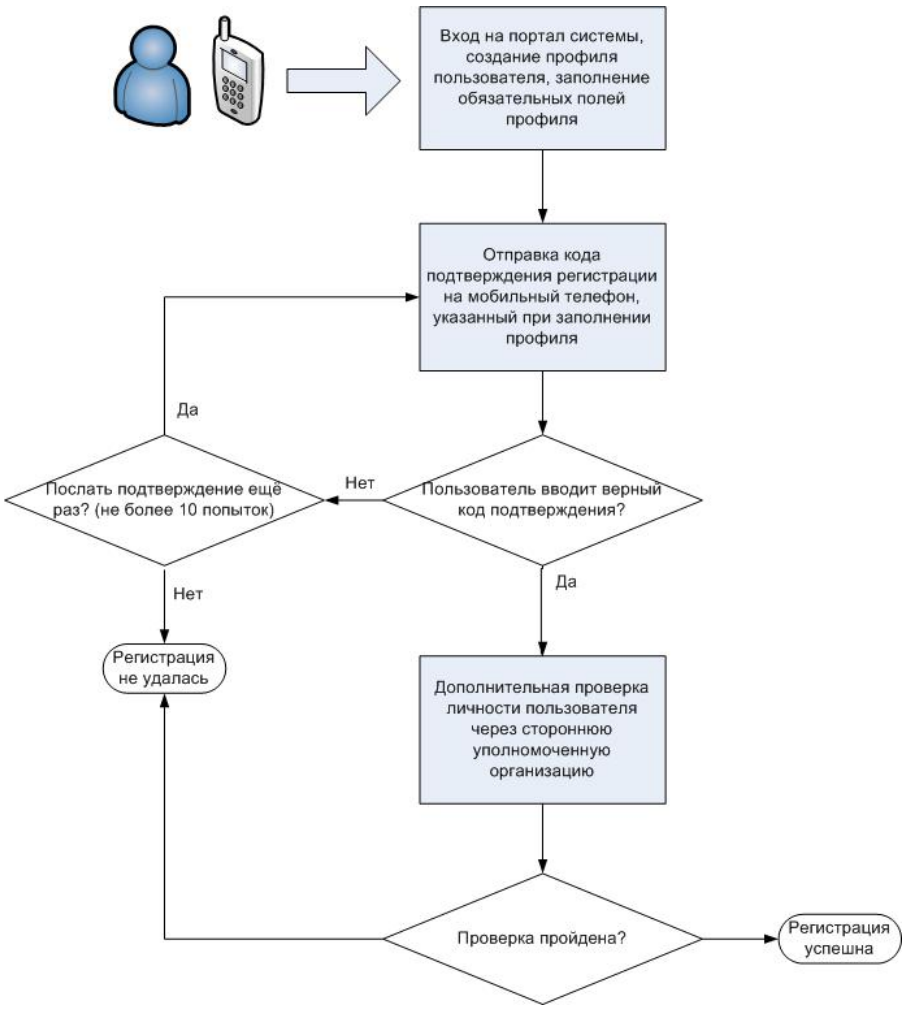


Рис. 2 Регистрация паспорта

Представленная процедура регистрации хорошо работает, когда есть возможность подтвердить подлинность паспорта через третью организацию. Однако в вырожденных случаях, когда у пользователя нет банковского счета она не может гарантировать полную достоверность полученных сведений.

В отсутствии банковского счета этом такая схема не исключает подлога фиктивного паспорта, формально соответствующего требованиям, которые предъявляют к паспорту считыватель, а также просто подмены отдельных страниц документа.

Таким образом предлагаемая схема без дополнительных проверок позволяет привязывать в системе:

– документы, заведомо не являющиеся паспортами гражданина РФ;

– заведомо поддельные документы.В этом случае предлагаются следующие меры, чтобы снизить вероятность

Чтобы снизить вероятность предоставления заведомо ложных сведений пользователем, используются следующие дополнительные процедуры при проверке получаемой информации:

– регистрация не только первого разворота паспорта, но и всех его остальных страниц;

– обязательное использование считывателей, дающих изображение в ультрафиолетовом свете;

– проверка личности пользователя через оператора мобильной связи, который по требованиям законодательства обязан идентифицировать абонентов;

– регистрация в системе дополнительного документа или какого-либо биометрического признака, например скана отпечатков пальцев пользователя.

Однако, несмотря на принимаемые дополнительные меры, использование данной схемы регистрации несет на себе ряд ограничений.

Регистрация документов.

Предложенная схема регистрации пользователей, позволяет осуществлять с ними различные юридически-значимые действия, которые имеют отражение не только в виртуальном пространстве, но и в реальной жизни. Одним из вариантов использования данных, полученных в результате такой процедуры регистрации, является способ юридически-значимой регистрации документов – электронная канцелярия.После регистрации паспорта в электронной услуге можно выстроить с

пользователем систему взаимодействия с использованием электронной подписи (ЭП), причем в данном случае не обязательно использование квалифицированной ЭП. С помощью неквалифицированной ЭП, при условии, что паспорт пользователя зарегистрирован и с ним заключен договор на оказание услуг, в котором прописан порядок использования неквалифицированной ЭП, можно осуществить регистрацию электронных документов, по следующей схеме:

Рис. 3 Заверение документа ЭП.

Заверение документа электронной печатью производится следующим образом:

1. Отправка документа через Интернет на сайт, выдающий электронные печати
2. Создание электронной печати на основе документа, времени его поступления на сайт (и идентификатора пользователя)
3. Размещение копий электронной печати в независимых хранилищах (на не модифицируемых носителях)
4. Передача пользователю копии электронной печати.

Заключение: практика применения электронной регистрации паспорта.

Процедура электронной регистрации паспорта разработана с целью максимального снижения рисков предоставления пользователем недостоверной инофрмации о своей личности и придания юридической значимости всем взаимодействиям с зарегистрированным пользователем.

Несмотря на то, что процедура регистрации использует несколько способов проверки информации, получаемой от пользователя, риск предоставления заведомо недостоверных сведений в некоторых случах все-таки остается. В этой связи разумно ограничить использование данной процедуры электронной регистрации паспорта, чтобы свести к минимуму риски организации, предоставляющей на основании полученной при регистрации информации, услуги. Чтобы снизить риски организации, предоставляющей услугу, предлагается:

– использовать процедуру электронной регистрации паспорта главным образом для услуг, в которых все риски, в т.ч. финансовые и юридические, от предоставления заведомо ложной информации, ложатся на пользователя услуги;

– включать ответственность пользователя за предоставление заведомо ложных сведений в договор на оказание услуг, заключаемый пользователем;

– использовать при регистрации и заключении договора с пользователем средства обеспечения юридической значимости такие, как электронная подпись [3];

– проверка документов визуально при первом личном обращении пользователя к оператору услуги: в этом случае пользователь может быть ограничен в возможностях внутри системы, до тех пор, пока не подвердит свои данные лично.

Рассмотренная в настоящей статье процедура регистрации успешно используется при предоставлении биржевых услуг. В этом сценарии биржевой брокер выступает для своих клиентов в т.ч. в роли налогового агента и для осуществления своих действий ему необходимы паспортные данные пользователей.

Использование электронной регистрации для биржевой торговли происходит следующим образом:

– пользователь проходит процедуру регистрации у брокера, регистрирует свой паспорт и остальные необходимые данные;

– после регистрации пользователю доступны все функции по использованию его биржевого счета, биржевые операции, уплата налогов и т.п.;

– как только пользователь в первый раз захочет вывести деньги со своего биржевого счета, ему будет предложено посетить офис брокера, либо вызвать курьера для подписания соответствующих документов;

– курьер или сотрудник брокера проводят визуальную сверку данных паспорта пользователя и данных предоставленных им в процессе регистрации, после чего пользователю больше не требуется личное общение с брокером, в дальнейшем достаточно электронного взаимодействия с использованием электронной подписи.

Использование процедуры электронной регистрации паспорта позволило существенно повысить поток клиентов, т.к. для начала работы с биржей не требуется визит в офис к брокеру. При этом меры проверки, используемые в процедуре регистрации позволили получить процент достоверных предоставляемых документов пользователей близкий в 100%. Планируется дальнейшее внедрение данной процедуры регистрации в организациях финансового сектора и банках.

СПИСОК ЛИТЕРАТУРЫ

1. Алексей Попов: «Электронный паспорт будет паспортом в реальном мире» [Электронный ресурс]. URL: http://www.uecard.ru/press/media-review/aleksey-popov-elektronnyy-pasport-budet-pasportom-v-realnom-mire/ (дата обращения 10.08.2013).
2. Горелик С.Л. и другие. Комплексное исследование вопросов обеспечения граждан Российской Федерации и органов государственной власти электронной почтовой связью. // Отчёт о научно-исследовательской работе. Шифр темы ЦА/05-10, № госрегистрации 01201065830.
3. Горелик С.Л., Ляпер В.С., Технологические подходы к обеспечению юридически значимого взаимодействия в облачных услугах //Информационные системы для научных исследований – 2012. – С. 274-279.
4. Горелик С.Л. Система дистанционной экспресс регистрации субъектов и документов // Заявка на патент № 2012109045, приоритет от 12.03.2012г. Решение о регистрации патента от 14.05.2012 г.
5. Горелик С.Л. (Проект "Честный интернет". Т.1.Система идентификации и аутентификации. Т.2. Система юридически значимых коммуникаций. Т.3. Электронная канцелярия и печать (Проект "Честный интернет") Научно-технический отчет по проекту «Честный интернет». // Свидетельство о регистрации: 07N-4R-RJ. Дата: 01.05.2011. Электронный регистратор «COPYTRUST». URL: https://www.copytrust.ru/.

УДК 002:004.056

АНАЛИЗ И ПРИМЕНЕНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ В SIEM-СИСТЕМАХ НА ОСНОВЕ ГРАФОВ АТАК И ЗАВИСИМОСТЕЙ СЕРВИСОВ[3]

Дойникова Елена Владимировна, Котенко Игорь Витальевич,
Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14-я линия В.О., д. 39,
e-mails: doynikova@comsec.spb.ru, ivkote@ comsec.spb.ru.

Аннотация: В данной работе рассматривается вычисление и применение показателей защищенности компьютерной системы (сети) для систем мониторинга и управления безопасностью (Security Information and Events Management, SIEM). На основе выделения нескольких аспектов оценивания (анализ атак и принимаемых контрмер, учет известных уязвимостей и уязвимостей «нулевого дня», расчет стоимостных и других показателей) и различных уровней представления компьютерной системы (топологический, графа атак, атакующего, событий и системы) сформирован подход к определению текущей ситуацию по безопасности. Предлагаемые в рамках подхода алгоритмы расчета показателей защищенности зависят от уровня представления компьютерной системы и режима функционирования SIEM-системы. Демонстрируется пример применения предложенной методики для сценария «Олимпийские Игры».

Ключевые слова*: системы мониторинга и управления безопасностью; показатели защищенности; оценивание риска; графы атак; графы зависимостей сервисов.*

ANALYSIS AND APPLICATION OF THE SECURITY METRICS ON THE BASE OF THE ATTACK GRAPHS AND SERVICE DEPENDENCIES GRAPHS FOR THE SIEM SYSTEMS

Doynikova Elena Vladimirovna, Kotenko Igor Vitalievich,
Saint-Petersburg institute for information and automation of RAS,
Russia, Saint-Petersburg, liniya 14-ya, 39,
e-mails: doynikova@comsec.spb.ru, ivkote@ comsec.spb.ru.

Abstract: The paper considers calculation and application of the security metrics for the computer systems (networks) for the Security Information and Events Management systems (SIEM-systems). The approach to the monitoring of the current security situation is formed on the base of the definition of the set of the

[3] Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417, 14-37-50735), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и государственных контрактов № 14.604.21.0033, 14.604.21.0137, 14.604.21.0147 и 14.616.21.0028.

assessment aspects (analysis of the attacks and selected countermeasures, consideration of the known vulnerabilities and zero-days, calculation of the cost metrics and other metrics) and different representation levels of the computer system (topological, attack graph, attacker, events and system). The algorithms for the calculation of the security metrics that are suggested in the approach are depend on the representation level of the computer system and operation mode of the SIEM-system. Application of the suggested technique for the “Olympic Games” case study is presented.

Keywords*: security information and event management; security metrics; risk assessment; attack graphs; service dependencies graphs.*

Введение. В результате увеличения объемов и разнородности информации, связанной с безопасностью, а также количества различных событий безопасности в рамках информационной инфраструктуры организаций, в последнее время активно развиваются технологии SIEM-систем [1 – 6]. Одной из важных функций SIEM-систем является предоставление информации о текущей ситуции по безопасности и поддержка принятия решений при реагировании на инциденты информационной безопасности. Для ее выполнения проводится вычисление и анализ соответствующих показателей защищенности.

В настоящий момент существует большое количество работ в области оценивания защищенности при помощи показателей, например [7 – 16]. Показатели, рассматриваемые в данных работах, можно разделить на следующие группы:

1. Топологические характеристики системы;
2. Характеристики атаки;
3. Характеристики атакующего;
4. Интегральные (системные) показатели, отражающие уровень защищенности системы в целом.

Топологические характеристики задаются на основе описания компьютерной сети, в том числе используя спецификации хостов, связей между ними, приложений и уязвимостей. Такие характеристики рассматриваются, например в [17] и [18]. Они позволяют выявить наиболее критичные и уязвимые объекты сети, однако не учитывают вероятность и последствия сложных многошаговых атак.

Характеристики многошаговых атак рассчитывается на основе графов атак [7], [8], [11], [14], [19] и графов зависимостей сервисов [20]. Графы атак обычно используются для определения характеристик атакующего [7], [8], [19], потенциала или вероятности атаки [7], [8], [11], [14]. Зависимости сервисов используются для расчета ущерба от атаки [9], [20].

Интегральные (системные) характеристики определяют общий уровень защищенности системы [7], [8], [11], [12 – 14].

Также следует выделить такие группы показателей, как стоимостные показатели [9], [12], позволяющие связать ущерб от атаки с потерями для бизнеса, и показатели, отражающие возможность атак нулевого дня [21], позволяющие учесть неизвестные уязвимости.

Однако традиционно для определения уровня защищенности системы используется только один из рассмотренных наборов характеристик (например, показатели возможного ущерба от атаки, на основе графов зависимостей сервисов, или показатели вероятности атаки, на основе графов атак). Кроме того, в текущих SIEM-системах обычно не используется механизм оценивания риска на основе анализа будущих и предшествующих действий атакующего, который позволяет более адекватно опредилить наиболее вероятные и опасные варианты развития обнаруженной атаки.

В данной работе описывается разработанный авторами подход к анализу защищенности, ориентированный на архитектуру SIEM-систем, основанный на ряде показателей защищенности, и позволяющий всесторонне отразить текущую ситуацию по безопасности с учетом различных входных данных (таких как описание системы, графы атак, графы зависимостей сервисов, инциденты безопасности), и при различных режимах функционирования системы (статическом и во времени, близком к реальному).

В статье также представлена реализация наиболее важных элементов подхода для сценария «Олимпийские Игры» [3].

Предложенный подход первоначально был разработан как часть решений по созданию SIEM-системы в проекте MASSIF (Management Security and information in Service Infrastructures) [3] и был реализован в рамках компонента моделирования атак и оценивания защищенности (Attack Modelling and Security Evaluation Component, AMSEC) [22].

Постановка задачи. Общая задача разработки подхода к анализу защищенности на основе показателей должна включать как минимум два этапа:

1. Выбор (разработка) общего подхода к оцениванию защищенности;
2. Определение показателей защищенности, которые с одной стороны учитывают все особенности выбранного подхода к оцениванию защищенности и, с другой стороны, могут предоставить эффективную оценку защищенности.

В рамках данной задачи были поставлены следующие основные подзадачи:

1. Классифицировать существующие работы и выделить наиболее значимые показатели защищенности, согласно информации, которую они могут предоставить пользователю (оператору) SIEM-системы;

2. Определить входные данные для расчета показателей защищенности и соответствующие алгоритмы расчета показателей;

3. Сделать процесс оценивания системы гибким, т.е. предоставить возможность пересчета показателей в зависимости от заданных условий (таких как режим функционирования системы, наличие исторических данных об инцидентах, знания об атакующем).

На основе поставленной задачи был определен ряд нижеуказанных функциональных требований к подходу оценивания защищенности:

– подход должен позволять осуществлять всеобъемлющую оценку рисков и помогать администратору по безопасности принять наиболее адекватное решение по реагированию с учетом временных и стоимостных требований;

– в статическом режиме подход должен позволять определить наиболее уязвимые и слабые места системы, позволять выявить возможные атаки, их вероятность и возможный ущерб в случае их успешной реализации, а также учитывать профиль атакующего при оценивании уровня защищенности системы (так как уровень навыков атакующего влияет на его возможность выполнить атакующее действия);

– в динамическом режиме подход должен позволять учитывать последние события в системе и переоценивать ситуацию по безопасности согласно полученным событиям;

– подход должен давать возможность оценить стоимость атак, стоимость ответных мер и выигрыш при реагировании для выбора наиболее эффективного решения по реагированию на инциденты безопасности;

– подход должен удовлетворять современным стандартам и протоколам в области информационной безопасностью.

Конечной целью решения данной задачи является предоставление пользователю системы всеобъемлющей, актуальной и адекватной инофомации по защищенности в виде ряда показателей защищенности.

Основные положения. Разработанный подход к оцениванию защищенности основан на многоуровневой системе показателей защищенности (таблица 1) и алгоритмах вычисления показателей каждого уровня, позволяющих уточнить оценку за счет новых входных данных.

Система показателей защищенности определяется особенностями функционирования компонента моделирования атак и оценивания защищенности AMSEC, такими как входные данные (модель анализируемой системы, модель атакующего и модель событий), способ представления входных данных на основе протокола «Автоматизации управления данными безопасности» (Security Content Automation Protocol, SCAP) [23], [24] и входящих в его состав стандартов (что определило применение стандарта «Общая система оценивания уязвимостей» (Common Vulnerabilities Scoring System, CVSS) [25] для оценивания уязвимостей), и результаты работы компонента (графы атак и графы зависимостей сервисов).

Также система определяется требованиями со стороны режимов функционирования SIEM-системы (статическим и динамическим) и результатами анализа релевантных работ в области показателей защищенности.

На основе всего перечисленного было определено несколько аспектов оценивания (анализ атак и принимаемых контрмер, учет известных уязвимостей и уязвимостей «нулевого дня», расчет стоимостных и нестоимостных показателей) и уровней представления компьютерной системы (топологический, в том числе с учетом правил разграничения доступа межсетевых экранов [26], уровень графа атак, уровень атакующего, уровень событий и уровень системы).

Каждый из этих аспектов и уровней определяет соответствующую группу показателей защищенности.

Эти показатели позволяют оценить топологию системы, характеристики атакующего и атаки, текущую ситуацию (путем обработки поступающих событий безопасности), интегральные характеристики защищенности и характеристики, основанные на стоимостном анализе и анализе уязвимостей нулевого дня.

В работе используются как показатели, заимствованные из релевантных работ, так и новые и модифицированные показатели.

Основная идея предлагаемого подхода состоит в разработке и использовании комплексной иерархической системы показателей, позволяющих адекватно, на разных уровнях и с учетом различных аспектов отразить текущий уровень защищенности. Часть рассматриваемых показателей используется для оценивания общего уровня защищенности системы, другие показатели отражают различные аспекты функционирования системы.

Таблица 1

Классификация показателей защищенности

Уровень	Входные данные	Показатели защищенности
Топологический	Модель системы (включая зависимости сервисов); Информация об уязвимостях/ слабых местах (включая индексы CVSS)	*Уязвимость хоста* *Слабость хоста* *Внутренняя критичность* *Внешняя критичность* *Процент систем без известных критичных уязвимостей* *Уязвимость хоста к атакам нулевого дня* *Ценность хоста для бизнеса*
Графа атак	Вся информация с предыдущего уровня; Графы атак	*Критичность атакующих действий* *Потенциал атаки* *Ущерб от атаки* *Потенциал атаки с учетом 0-дня* *Стоимостной ущерб от атаки* *Затраты на реагирование*
Атакующего	Вся информация с предыдущего уровня; Профиль атакующего (навыки, местоположение в системе, уровень привилегий)	*Уровень навыков атакующего* *Профильный потенциал атаки* *Профильный потенциал атаки с учетом 0-дня* *Профильный стоимостной ущерб от атаки* *Профильные затраты на реагирование*
Событий	Вся информация с предыдущего уровня; Инциденты безопасности	*Позиция атакующего* *Динамический уровень навыков атакующего* *Вероятностный уровень навыков атакующего* *Динамический потенциал атаки* *Динамический потенциал атаки с учетом 0-дня* *Динамический стоимостной ущерб от атаки* *Динамические затраты на реагирование*
Интегральный (системы)	Показатели предыдущих уровней	*Уровень риска* *Уровень защищенности* *Поверхность атаки*

Показатели топологического уровня определяются администратором на основе топологии системы (сети). Основные показатели топологического уровня приведены в таблице 1. Для оценивания интегрального показателя уровня риска на данном уровне используются показатели критичности хоста, ущерба от успешной эксплуатации уязвимости (основан на индексе CVSS «Ущерб» (Impact)) и вероятности успешной эксплуатации уязвимости (основан на индексе CVSS «Возможность использования» (Exploitability)). Другие показатели предоставляются администратору в качестве дополнительной информации. В этой связи, остановимся подробнее на показателе критичность хоста. Методика вычисления данного показателя включает следующие этапы:

1. Выделение различных приложений хоста application_1, application_2, …, application_m;

2. Определение критичности каждого приложения согласно важности его конфиденциальности, целостности и доступности (CIA) для системы на основе экспертных оценок владельцев активов (критичность Cc относительно конфиденциальности, критичность Ci относительно целостности и критичность Ca относительно доступности), и выбор только тех приложений, которые критичны для системы;

3. Вычисление двух видов критичности приложения – внутренней (т.е. критичности собственно приложения для системы) и внешней (т.е. критичности приложения для корректной работы других приложений). Например, доступность приложения application_2 может быть критична для конфиденциальности, целостности или доступности приложения application_1 (с соответствующими весовыми коэффициентами). Это определяется с помощью матрицы 3x3 (влияние каждого свойства одного приложения на каждое свойство другого приложения). Таким образом, внешняя критичность приложения application_2 определяется на основе произведения внутренней критичности приложения application_1 на весовую матрицу (данный подход основан на способе вычисления внешнего ущерба в [20]):

$$E_Criticality_{ap_2} = W_{ap_1,ap_2} \times I_Criticality_{ap_1}, \quad (1)$$

где

W_{ap_1,ap_2} - весовая матрица;

$I_Criticality_{ap_1}$ - внутренняя критичность приложения application_1.

4. Расчет критичности хоста на основе трех оценок (для конфиденциальности, целостности и доступности). Каждая оценка определяется как максимальная из внутренних и внешних критичностей для всех приложений хоста [20]:

$$H_Criticality = \begin{bmatrix} \max_k Criticality_k(c) \\ \max_k Criticality_k(i) \\ \max_k Criticality_k(a) \end{bmatrix}, \quad (2)$$

где k - количество приложений хоста, $k \in [1..m]$;

$Criticality_k(c) = \max(I_Criticality(c), E_Criticality(c))$;

$Criticality_k(i) = \max(I_Criticality(i), E_Criticality(i))$;

$Criticality_k(a) = \max(I_Criticality(a), E_Criticality(a))$.

На уровне графа атак для вычисления показателей защищенности используется информация, получаемая на основе графа атак. Данный уровень позволяет определить вероятность атаки и возможный ущерб с учетом всех путей атаки.

Потенциал атаки может определяться несколькими способами: статически или динамически. В работе применяется модификация подхода, предложенного в [11]. В данном случае используются вероятность успешного использования уязвимостей, вычисляемая на основе показателей CVSS, и теорема Байеса:

– каждое состояние определяется как успешная или неуспешная эксплуатация уязвимостей, соответствующих узлу графа атак, и ведущая к достижению определенных постусловий;

– вероятность перехода от одного узла к другому определяется сложностью доступа к соответствующей уязвимости (если существует несколько уязвимостей, ведущих к данному состоянию, то вероятность определяется минимальной сложностью доступа):

$$Pr(e_i) = CVSS_AC, \quad (3)$$

где $CVSS_AC$ - сложность доступа CVSS; e_i - используемая уязвимость;

- для каждого узла вычисляются локальные распределения вероятностей. На их основе находятся безусловные вероятности состояний по формуле совместного распределения вероятностей: для набора состояний $S = \{S_1, ..., S_n\}$:

$$\Pr(S_1, ..., S_n) = \prod_{i=1}^{n} \Pr(S_i \mid \mathrm{Pa}[S_i]), \quad (4)$$

где $\mathrm{Pa}[S_i]$ - последовательность всех узлов, предшествующих S_i [11].

Ущерб от атаки определяется на основе непосредственного ущерба, наносимого атакующим действием (непосредственный ущерб), и критичности хоста.

Непосредственный ущерб статически определяется на основе вектора {ущерб конфиденциальности, ущерб целостности, ущерб доступности}, который может быть рассчитан с использованием показателей CVSS для уязвимостей, используемых в атакующем действии: (I_c, I_i, I_a), где I_c – ущерб конфиденциальности, I_i - ущерб целостности, I_a - ущерб доступности.

Ущерб от атаки вычисляется перемножением непосредственного ущерба и критичности хоста.

Для оценивания интегрального показателя уровня риска на данном уровне перемножаются показатели ущерб от атаки и потенциала атаки.

На уровне атакующего вводится зависимость от профиля атакующего (т.е. его положения в сети и навыков). Это позволяет сформировать так называемый профильный граф атак [19], который включает атаки, которые может реализовать именно данный атакующий. К основным показателям данного уровня относятся уровень навыков атакующего и профильный потенциал атаки. Уровень навыков атакующего определяется статически администратором как Низкий/Средний/Высокий. На основе данного показателя перерассчитывается потенциал атаки, формируя новый показатель профильный потенциал атаки.

Уровень событий соответствует динамическому режиму работы SIEM-системы. Он позволяет отслеживать развитие атаки и профиль атакующего по инцидентам безопасности. На основе поступающих событий корректируется позиция атакующего на графе атак и возможные пути продолжения атаки. Основными показателями уровня событий являются динамический уровень навыков атакующего, вероятностный уровень навыков атакующего, динамический потенциал атаки.

Динамический уровень навыков атакующего вычисляется динамически на основе максимальной сложности из реализованных атакующим шагов [8].

Вероятностный уровень навыков атакующего определяется на основе вероятностной методики с учетом сложности реализованных шагов и исторических данных.

Динамический потенциал атаки определяется на основе потенциала атаки предыдущего уровня с учетом инцидентов безопасности. При возникновении инцидента, вероятности состояний пересчитываются на основе теоремы Байеса, т.е. апостериорная вероятность для узла А, с учетом того, что событие, соответствующее узлу В произошло, определяется по формуле [11]:

$$Pr(A \mid B) = Pr(B \mid A) \times Pr(A) / Pr(B), \quad (5)$$

где $Pr(B)$, $Pr(A)$ - априорные безусловные вероятности узлов B и A.

Наконец, на уровне системы определяются общий уровень защищенности системы, для этого используется показатель - уровень защищенности. уровень защищенности применяется для определения общего состояния защищенности системы как риска того, что система будет скомпрометирована. Данный показатель определяется на основе потенциала атаки, ущерба от атаки и критичности хоста атакуемых хостов.

Пример применения. В качестве примера применения данного подхода рассмотрим процесс вычисления показателей ущерба от атаки и вероятности атаки, а также их динамического перерасчета в процессе функционирования системы в рамках сценария «Олимпийские Игры».

Рассмотрим вычисление показателей для следующих путей атаки, представленных на рис.1:

1. Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Massif-I;
2. Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Massif-I → Massif-1;
3. Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Massif-I → Massif-2.

Для определения *критичности хоста* владельцем ресурса задается внутренняя критичность хостов Massif-I, Massif-1 и Massif-2, а администратором задается весовая матрица для определения внешней критичности. Т.о. по формуле (1) внешняя критичность для хоста Massif-I определяется как:

$$E_Criticality_{Massif-I} = W_{Massif-I,\text{Massif}-1} \times I_Criticality_{Massif-1} + W_{Massif-I,\text{Massif}-2} \times I_Criticality_{Massif-2} =$$

$$= 2 \times \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0,8 \\ 0 & 0 & 0,8 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0,8 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1,6 \\ 1,6 \end{bmatrix}.$$

Критичность хоста Massif-I определяется по формуле (2) как:

$$H_Criticality = \begin{bmatrix} 0 \\ 1,6 \\ 1,6 \end{bmatrix}.$$

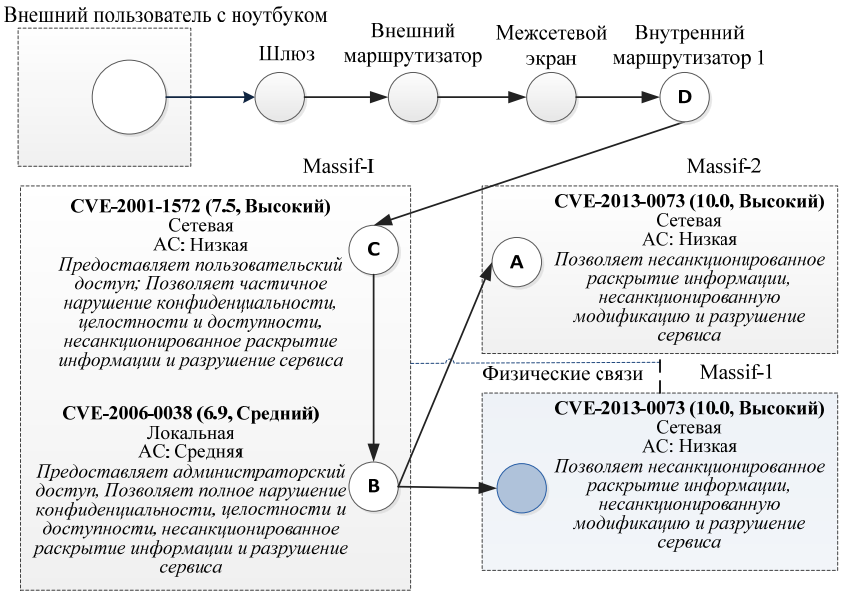


Рис. 1. Пример путей атаки

Определим потенциал атаки (на уровне графа атак) для путей атаки (1) – (3), представленных на рис.1. Определим узлы, соответствующие использованию уязвимостей данных путей следующим образом: A - CVE-2013-0073; B - CVE-2006-0038; C - CVE-2001-1572; D - Атакующий 1.

Вероятности успешного использования уязвимостей атакующим на основе формулы (3) определяются следующим образом:

$$Pr(e_A) = 0,71;\ Pr(e_B) = 0,61;\ Pr(e_C) = 0,71.$$

На основе локальных распределений условных вероятностей (определяемых на основе вероятности успешного использования соответствующих уязвимостей) определим безусловные вероятности для каждого узла, используя определение совместного распределения вероятностей (4). Для узла D есть только одно успешное состояние:

$$Pr(D) = 1.$$

Для узла C необходимо учесть успех на узле D:

$$Pr(C) = 1 \cdot 0,71 = 0,71.$$

Для узла B необходимо учесть успех на узле C:

$$Pr(B) = 0,71 \cdot 0,61 = 0,4331.$$

Для узла A необходимо учесть успех на узле B:

$$Pr(A) = 0,4331 \cdot 0,71 = 0,3075.$$

Таким образом, потенциал атаки для узла Massif-I равен $Pr(B) = 0,4331$. Потенциал атаки для узла Massif-1 равен потенциалу атаки для узла Massif-2 и равен $Pr(A) = 0,3075$.

Если дополнительно определить уровень навыков атакующего для Атакующего 1 как «Средний» (количественно определяется как 0,5). Тогда. исходная вероятность атаки на узел D: $Pr(D) = 0,5$.

Остальные оценки изменятся следующим образом: для узла D:

$$Pr(D) = 0,5.$$

Для узла C:

$$Pr(C) = 0,5 \cdot 0,71 = 0,355.$$

Для узла B:

$$Pr(B) = 0,355 \cdot 0,61 = 0,2166.$$

Для узла A:

$$Pr(A) = 0,2166 \cdot 0,71 = 0,1538.$$

Т.о. очевидно, что снижение уровня навыков атакующего ведет к снижению вероятности атаки на узел A.

Профильный потенциал атаки для узла Massif-I равен $Pr(B) = 0,2166$. Профильный потенциал атаки для узла Massif-1 равен профильному потенциалу атаки для узла Massif-2 и равен $Pr(A) = 0,1538$.

Ущерб от атаки для узла Massif-I определяется максимальным ущербом от использования уязвимостей хоста: CVE-2001-1572 - $[0,275 \quad 0,275 \quad 0,275]$ (значения для частичного ущерба согласно CVSS) и CVE-2006-0038 - $[0,660 \quad 0,660 \quad 0,660]$ (значения для полного ущерба согласно CVSS). Ущерб от атаки для узла: $[0,660 \quad 0,660 \quad 0,660]$.

Учитывая рассчитанную выше критичность хоста, общий ущерб от компрометации хоста для системы:

$$Attack_Impact = Attack_Impact \times H_Criticality = [0,660 \quad 0,660 \quad 0,660] \times \begin{bmatrix} 0 \\ 1,6 \\ 1,6 \end{bmatrix} = 2,112.$$

Ущерб от атаки для узла Massif-1 определяется максимальным ущербом от использования уязвимости хоста: CVE-2013-0073 - $[0,660 \quad 0,660 \quad 0,660]$ (значения для полного ущерба согласно CVSS). Ущерб от атаки для хоста: $[0,660 \quad 0,660 \quad 0,660]$. Далее, учитывая критичность хоста, рассчитанную выше, общий ущерб от компрометации хоста для системы:

$$Attack_Impact = Attack_Impact \times H_Criticality = [0,660 \quad 0,660 \quad 0,660] \times \begin{bmatrix} 1 \\ 0,8 \\ 1 \end{bmatrix} = 1,848.$$

Ущерб от атаки для пути (2), определяемый как сумма ущерба от атаки для Massif-I и Massif-1, равен 3,96. Таким образом, видно, что ущерб растет с продвижением атакующего в глубь сети.

Предположим, что поступил инцидент безопасности об успешной компрометации узла B. Пересчитаем потенциал атаки на основе теоремы Байеса, чтобы получить динамический потенциал атаки на уровне событий. Определим апостериорную вероятность для узла C, с учетом того, что B произошло по формуле (5):

$Pr(B) = 0,2166$, $Pr(C) = 0,355$ (вычислено раньше);

$Pr(B \mid C) = 0,61$;

$$Pr(C \mid B) = 0,61 \times \frac{0,355}{0,2166} = 0,9999.$$

Таким образом, вероятность C значительно возросла, при условии того, что B произошло (т.е. атакующий скорее всего скомпрометировал узел C, чтобы скомпрометировать узел B). Кроме того, с учетом того, что B произошло, изменится вероятность того, что произойдет A, так как теперь $Pr(B) = 1$, $Pr(A) = 1 \cdot 0,71 = 0,71$.

На рис.2 показаны изменения потенциала атаки, ущерба от атаки и уровня риска для узла B пути атаки (1) и узла A пути атаки (2) (см. рис.1) при добавлении информации на различных уровнях показателей защищенности.

Новая информация об уровне навыков атакующего снижает значение показателя, так как атакующий не может использовать все уязвимости (из-за недостатка знаний), также снижается и относительная величина уровня риска. На уровне событий значение обоих показателей растет из-за обнаружения нового события. Это позволяет делать предположения о предыдущих и последующих шагах атаки (с учетом критичности хостов на пути атакующего).

Также на основе сложности предыдущих шагов и направления атаки можно делать предположения об уровне знаний атакующего.

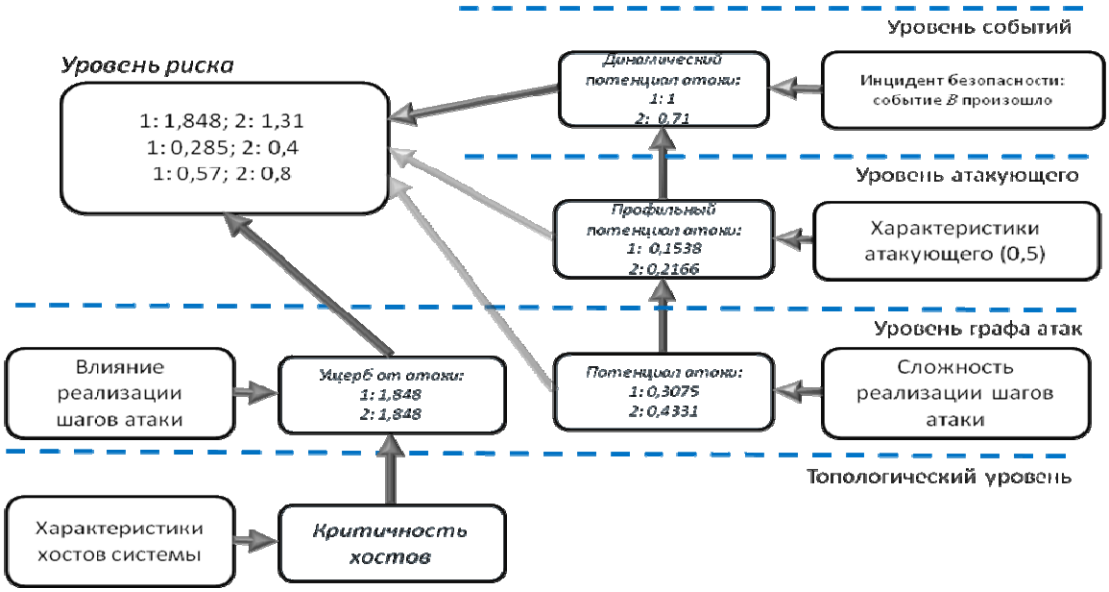


Рис. 2. Изменения значений потенциала атаки, ущерба от атаки и уровня риска

Заключение. В статье представлен подход к оцениванию защищенности в SIEM-системах, который позволяет учитывать профили атакующих, последовательности возможных атакующих действий в системе и инциденты безопасности. Предложена система показателей защищенности с учетом архитектуры и режимов работы SIEM-системы. Система содержит несколько уровней показателей, соответствующих различным входным данным (модель системы, модель атакующего, модель атаки, модель событий), что позволяет пересчитывать показатели на основе новой информации. Подход позволяет оценивать каждый элемент отдельно, а также использовать полученные оценки при оценивании общего уровня защищенности системы на основе предлагаемых методик. Методики выбраны в соответствии с последними исследованиями в области показателей защищенности. Более детальная информация приводит к более точным результатам оценки. Также в работе продемонстрирован пример перерасчета некоторых показателей для сценария «Олимпийские Игры». На данный момент не учитывается надежность данных, содержащихся в инцидентах безопасности. Однако это планируется учесть в будущих исследованиях.

В будущих планах также расширить набор показателей защищенности, детализировать описанные методики оценки защищенности, а также продолжить анализ эффективности методик на реальных примерах.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах //Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. С. 27–56.
2. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management //Proceedings of the International Conference on Security and Cryptography (SECRYPT 2012), Rome, Italy, 24-27 July 2012. P. 391–394.
3. MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures. http://www.massif-project.eu.
4. Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности //Системы высокой доступности, Т.8, № 2, 2012. С. 100–108.

5. Kotenko I., Polubelova O., Saenko I. The Ontological Approach for SIEM Data Repository Implementation //Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012 2012. P. 761–766.
6. Kotenko I., Polubelova O., Saenko I. Data Repository for Security Information and Event Management in Service Infrastructures //SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography. Rome, Italy. 24-27 July 2012. P. 308–313.
7. Jahnke M., Thul C., Martini P. Graph-based metrics for intrusion response measures in computer networks //Proceedings of the 3rd IEEE Workshop on Network Security, held in conjunction with 32th IEEE Conference on Local Computer Networks. Dublin, 2007.
8. Kanoun W., Cuppens-Boulahia N., Cuppens F., Araujo J. Automated reaction based on risk analysis and attackers skills in intrusion detection systems //Proceedings of the third International Conference on Risks and Security of Internet and Systems (CRiSIS'08). Toezer, Tunisia, 2008. P. 117–124.
9. Kheir N., Debar H., Cuppens-Boulahia N., Cuppens F., Viinikka J. Cost evaluation for intrusion response using dependency graphs //Proceedings of the International Conference on Network and Service Security, 2009. P. 1–6.
10. Manadhata P.K., Wing J.M. An attack surface metric //IEEE Transactions on Software Engineering, 2010. P. 371–386.
11. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using Bayesian attack graphs //IEEE Transactions on Dependable and Security Computing, 2012. Vol.9, No.1. P. 61–74.
12. Stakhanova N., Basu S., Wong J. A cost-sensitive model for preemptive intrusion response systems //Proceedings of the 21st International Conference on Advanced Networking and Applications, Washington, DC, USA, IEEE Computer Society, 2007. P. 428–435.
13. Wu Y.-S., Foo B., Mao Y.-C., Bagchi S., Spafford E.H. Automated adaptive intrusion containment in systems of interacting services //Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007. Vol.51. P. 1334–1360.
14. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior //SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P. 339–344.
15. Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В. Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов //Информационные технологии, № 1, 2009. С. 37–42.
16. Gorodetsky V., Kotenko I., Karsayev O. Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning //The International Journal of Computer Systems Science and Engineering, 2003, T.18, № 4. C. 191–200.
17. The Center for Internet Security, The CIS Security Metrics, 2009.
18. Mayer A. Operational Security Risk Metrics: Definitions, Calculations, Visualizations //Metricon 2.0. CTO RedSeal Systems, 2007.
19. Dantu R., Kolan P., Cangussu J. Network risk management using attacker profiling //Security and Communication Networks, 2009. Vol.2, No.1. P. 83–96.
20. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A service dependency model for cost-sensitive intrusion response //Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), 2010. P. 626–642.
21. Wang L., Singhal A., Jajodia S., Noel S. k-zero day safety: measuring the security risk of networks against unknown attacks //Proceedings of the 15th European conference on Research in computer security, Springer-Verlag Berlin, Heidelberg, 2010. P. 573–587.
22. Kotenko I., Chechulin. A. A Cyber Attack Modeling and Impact Assessment framework //Proceedings of the 5th International Conference on Cyber Conflict 2013 (CyCon 2013), Tallin, Estonia , 4-7 June 2013. P. 1–24.
23. Котенко И.В., Дойникова Е.В. Анализ протокола автоматизации управления данными безопасности SCAP //Защита информации. Инсайд, 2012, № 2. С. 56–63.
24. Waltermire D., Quinn S., Scarfone K., Halbardier A. The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2. September 2011.
25. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007.
26. Kotenko I., Polubelova O. Verification of Security Policy Filtering Rules by Mjdel Checking //Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2011), 2011. P. 706–710.

УДК 519.688

МЕТОД КОМПОЗИЦИИ ЧАСТНЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ В ЗАДАЧЕ ТИПИЗАЦИИ СИТУАЦИЙ В УПРАВЛЕНИИ ТЕЛЕКОММУНИКАЦИОННЫМИ СИСТЕМАМИ

Ковалев Илья Гаврилович,
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков, д 22, к.1,
e-mail: mail.kovalev@gmail.com.

Аннотация: Рассматривается использование метода ситуационного управления для решения задач оперативно-технического управления телекоммуникационными системами. Результатом применения метода является выделение классов ситуаций на основе полезностных показателей функционирования телекоммуникационной системы.

Ключевые слова: *управление; телекоммуникационная система; ситуационное управление; классификация ситуаций; характеристика системы; показатель эффективного функционирования системы*

THE METHOD OF COMPOSITION INDIVIDUAL PERFORMANCE INDICATORS IN THE TASK TYPING SITUATIONS IN THE MANAGEMENT OF TELECOMMUNICATION SYSTEMS

Kovalev Ilya,
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov, 22-1,
e-mail: mail.kovalev@gmail.com.

Abstract: Discusses the use of the method of situational management for solving tasks of the operational-technical management of telecommunication systems. The result of this method is the selection of classes of situations on the basis of indicators usefulness of functioning telecommunications system.

Keywords: *management; a telecommunication system; case management; classification of situations; characteristic of the system; indicator of the effective functioning of the system*

Введение. В настоящее время общепринятым аппаратом оценки сложных систем являются модель динамической системы и теория полезности, позволяющие определить важные для ЛПР характеристики системы на основе формальной модели процесса. Одновременно с ними широко используются эвристические методы оценки (и управления), наиболее развитым из которых следует признать метод ситуационного управления [1].

Одной из наиболее актуальных задач эффективного совместного использования этих методов для решения задач оперативно-технического управления телекоммуникационными системами (ТС) является выделение классов ситуаций на основе полезностных показателей функционирования ТС.

Постановка и решение задачи.

Анализ проблем реализации ситуационного метода в управлении телекоммуникационными системами [2], позволяет считать целесообразным определение ситуации на основе базовой модели (МОТ-модели) [3], реализующей единообразное представление структуры физических процессов электросвязи с учетом международных рекомендаций по архитектуре управления (TMN, eTOM) и организационно-техническому признаку как ведущих феноменов управления телекоммуникационными системами.

Графическая интерпретация МОТ-модели представлена на рисунке 1.

Рассматриваются различные интерпретации телекоммуникационной системы, представляющие собой описание некоторого процесса, представленного моделью (СМО, взвешенный граф или модели линии связи), реализующего функционал некоторой службы, в составе организационной единицы.

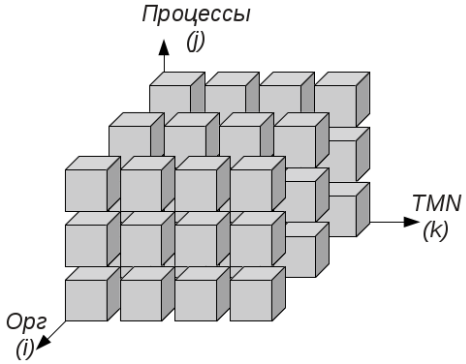


Рис. 1. Пространство дискрет МОТ-модели

Орту организационного представления, для удобства интерпретации, будем рассматривать от «начала отсчета»: узел, филиал, компания. Аналогично для орты процессов: энергетический обмен (ЭО), транспортный обмен (ТО), информационный обмен (ИО); и орты служб (TMN): объекты, сети, услуги, бизнес.

Каждая из дискрет МОТ-модели предполагает наличие формальной модели (из класса моделей по орте процессов), по которой рассчитываются показатели, определяемые зоной ответственности, определяемой уровнем организационной иерархии и формой представления в терминах TMN-архитектуры.

Предположим, что для каждой дискреты вычисляется показатель эффективности (частный показатель эффективности, ЧПЭ), характеризующий степень достижения системой поставленных целей, то есть учитывающий в оценке системы ценности ЛПР.

В рассматриваемой модели интерес представляют, прежде всего, взаимосвязи между ЧПЭ. Для их описания исходное множество ЧПЭ будем рассматривать как объединение одноэлементных подмножеств

$$A = \bigcup_{ijk} \{J_{ijk}\}, \quad J_{ijk} = \varphi_E(D_{ijk}), \tag{1}$$

где J_{ijk} - ЧПЭ дискреты D_{ijk},

φ_E - процедура оценки ЧПЭ.

Для простоты будем рассматривать единственную порядковую шкалу $Q = \{r, y, g\}$, $r \prec y \prec g$, где строчные буквы означают соответственно цвета «красный», «желтый» и «зеленый», отражающие оценку системы, представленной соответствующим классом интерпретации.

Определим структуру на множестве дискрет МОТ-модели как булеан множества дискрет МОТ-модели с заданной на нем алгеброй подмножеств:

$$\left\langle 2^{\{D_{ijk}\}}, \{\cup, \cap, -\} \right\rangle \tag{2}$$

В соответствии семантикой МОТ-модели, возможно образование подмножеств дискрет (ЧПЭ) посредством операций (2), изображенных на рисунке 2

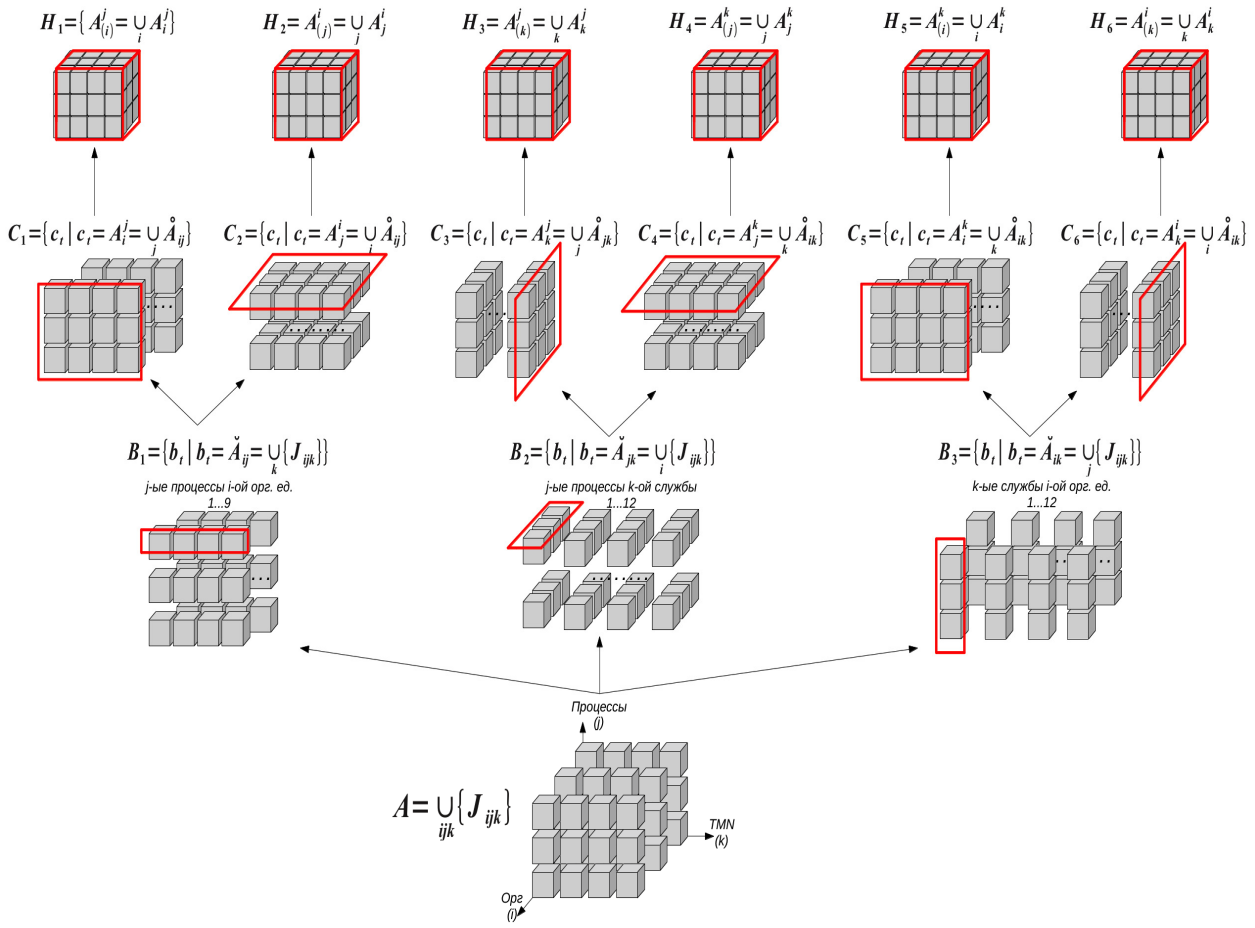


Рис. 2. Подмножества дискрет-ЧПЭ

Булеан (2) гомоморфно отображаемый на множество ЧПЭ позволяет определить на множестве ЧПЭ порядок по включению $A \le B_l \le C_m \le H_n$ в том смысле, что элемент каждого множества определяется как некоторая совокупность единичных ЧПЭ:

$$[card(J_{ijk}) = J_{ijk} = 1] < \left[card(b_t) = \begin{cases} \dot{A}_{jk} = \bigcup_i \{J_{ijk}\}, 3 \\ \dot{A}_{ik} = \bigcup_j \{J_{ijk}\}, 3 \\ \dot{A}_{ij} = \bigcup_k \{J_{ijk}\}, 4 \end{cases} \right] < \left[card(c_t) = \begin{cases} \bigcup_j \dot{A}_{ij}, 4\times 3 \\ \bigcup_i \dot{A}_{ij}, 4\times 3 \\ \bigcup_j \dot{A}_{jk}, 3\times 3 \\ \bigcup_k \dot{A}_{ij}, 3\times 3 \\ \bigcup_i \dot{A}_{ik}, 3\times 3 \\ \bigcup_k \dot{A}_{ik}, 3\times 3 \end{cases} \right] <$$

$$< [card(H_n) = 36]$$

Указанное отношение порядка позволяет сформировать классы ситуаций по признаку масштаба – количества вовлеченных дискрет: $\{A, B, C, H\}$.

Среди множеств второго уровня декомпозиции (*C*), можно выделить эквивалентные по включению элементов предыдущего уровня (*B*), абстрагируясь от типа элементов множеств (B_i), их составляющих: $C_1 \sim_J C_5$, $C_2 \sim_J C_4, C_3 \sim_J C_6$. Характерной особенностью этих эквивалентных множеств является то, что их элементы представляют собой «срез» МОТ-модели по одной из орт.

Для множеств $C_1 \sim_J C_5$ (аналогично для остальных):

$$c_t^1 = \bigcup_j \dot{A}_{ij} = \bigcup_j (J_{ij1} \cup J_{ij2} \cup J_{ij3} \cup J_{ij4}) =$$

$$= (J_{i11} \cup J_{i12} \cup J_{i13} \cup J_{i14}) \cup (J_{i21} \cup J_{i22} \cup J_{i23} \cup J_{i24}) \cup (J_{i31} \cup J_{i32} \cup J_{i33} \cup J_{i34}) =$$

$$= J_{i11} \cup J_{i12} \cup J_{i13} \cup J_{i14} \cup J_{i21} \cup J_{i22} \cup J_{i23} \cup J_{i24} \cup J_{i31} \cup J_{i32} \cup J_{i33} \cup J_{i34} =$$

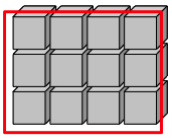
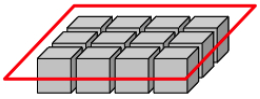
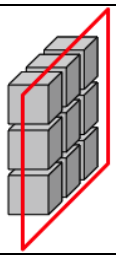
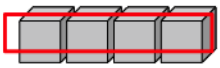
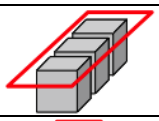
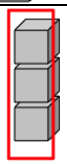
$$= (J_{i11} \cup J_{i21} \cup J_{i31}) \cup (J_{i12} \cup J_{i22} \cup J_{i32}) \cup (J_{i13} \cup J_{i23} \cup J_{i33}) \cup (J_{i14} \cup J_{i24} \cup J_{i34}) =$$

$$= \bigcup_k (J_{i1k} \cup J_{i2k} \cup J_{i3k}) = \bigcup_k \dot{A}_{ik} = c_t^5$$

Таким образом, в каждом классе ситуаций можно выделить типы ситуаций по отношению эквивалентности $\sim_J$.Элемент конкретного множества некоторого уровня декомпозиции и способ его формирования характеризуют локализацию ситуации. Полученная классификация приведена в таблице 1 и на рисунке 3.

Таблица 1

Типы ситуаций

Тип ситуации	Способ формирования	Физический смысл
		Комплексные нарушения функционирования
	B1	Нарушение инфраструктуры взаимодействия служб ххххх организационной единицы
	B3	Нарушение инфраструктуры поддержки физических процессов ххххх организационной единицы
	B1	Нарушение инфраструктуры взаимодействия служб в области процесса ххххх обмена
	B2	Нарушение инфраструктуры взаимодействия организационных единиц в области процесса ххххх обмена
	B2	Нарушение инфраструктуры ххххх службы по поддержке физических процессов
	B3	Нарушение инфраструктуры взаимодействия организационных единиц в области ххххх службы
	$\bigcup_k \{J_{ijk}\}$ $F(J_{ijk}, J_{lmn})$	Выявлены зависимости, свидетельствующие о функциональ-ной зависимости служб или конфликте интересов/ресурсов служб
	$\bigcup_k \{J_{ijk}\}$ $F(J_{ijk}, J_{lmn})$	Выявлены зависимости, свидетельствующие о функциональной зависимости служб или конфликте интересов/ресурсов служб
	$\bigcup_k \{J_{ijk}\}$ $F(J_{ijk}, J_{lmn})$	Выявлены зависимости, свидетельствующие о дисбалансе требований/обеспечения в структуре показателей физических процессов
	$J_{ijk} = [\Phi(L_r) \to Q]$	Существенные отклонения состояния динамической системы.

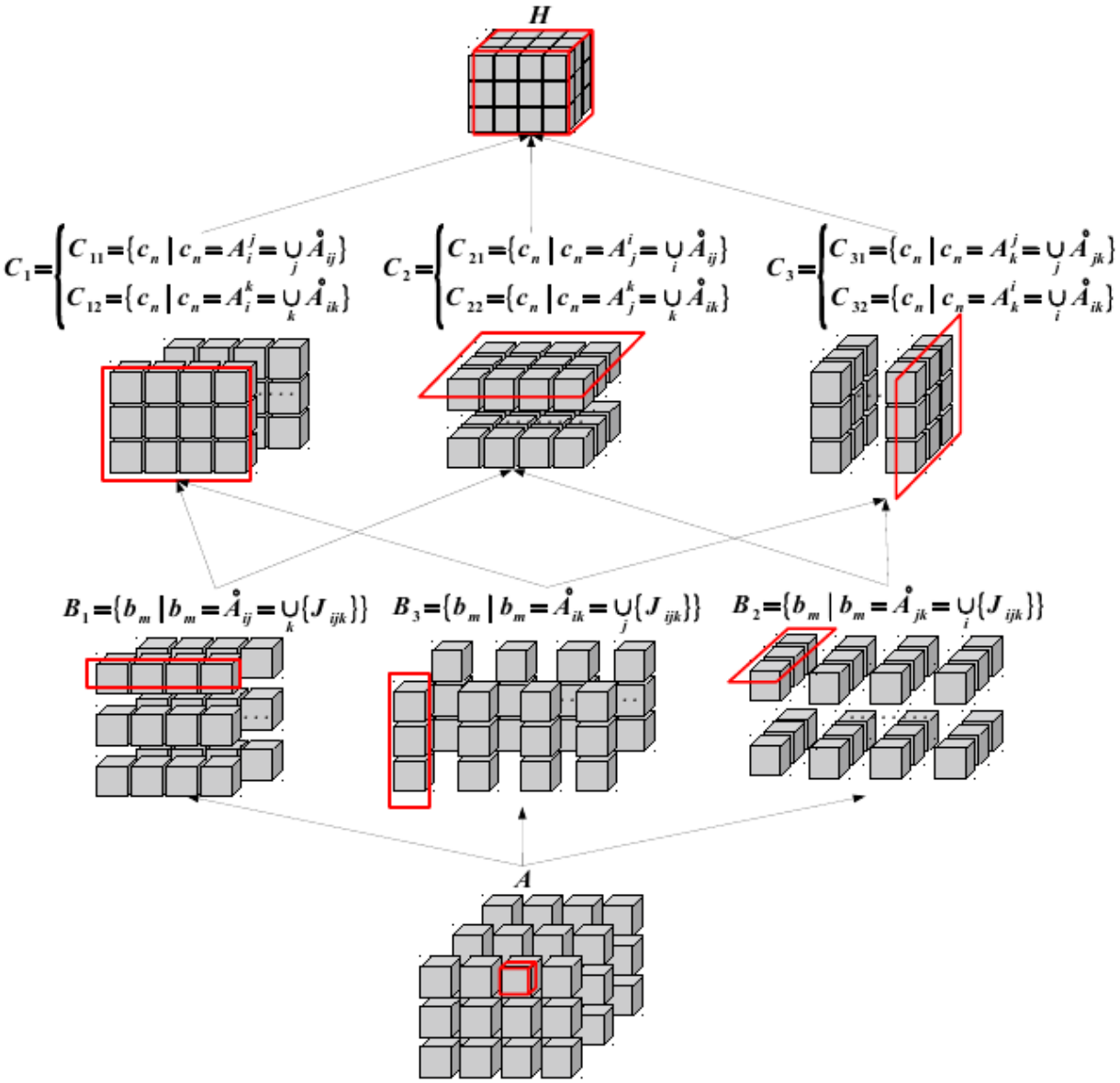


Рис. 3. Типы ситуаций

На базе приведенного метода композиции ЧПЭ может быть предложен метод классификации ситуаций на основе изучения отношений в базовой модели. Основными этапами построения классификатора тогда являются:

– введение алгебры подмножеств на множестве дискрет МОТ-модели;
– исследование подмножеств дискрет МОТ-модели;
– построение классов ситуаций в соответствии с отношением порядка по включению на элементах булеана дискрет МОТ-модели.

Заключение. Полученный на основе этих данных классификатор позволяет сформировать иерархическое описание ситуации, однако содержит элемент неопределенности, заключающийся как в механизме обобщения ситуаций (целесообразность рассмотрения ситуации конкретного класса), так и распознавании нескольких ситуаций одного типа в некотором классе (равномощных подмножеств одного класса, отличающихся способом формирования), и, отдельно, – определение локализации (конкретного элемента в каждом типе).

Исследование методов построения полноценного классификатора ситуаций на основе полученных результатов представляется перспективным направлением дальнейших исследований и развития методов ситуационного управления.

СПИСОК ЛИТЕРАТУРЫ

1. Поспелов, Д.А. Ситуационное управление: теория и практика / Д.А. Поспелов. – М.: Наука, 1986. - 288 с.
2. Ковалев, И.Г. Анализ проблем реализации ситуационного подхода к управлению телекоммуникационными системами / И.Г. Ковалев // 65-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов: материалы / ГОУВПО СПб ГУТ. — СПб.: 2012 — С. 56-58
3. Дадаев, В.И. Открытая базовая иерархическая модель телекоммуникационной системы / В.И. Дадаев, М.В. Фёдоров, С.О. Бурлаков // Информационные технологии моделирования и управления. — 2005. — №3. — С. 422-427

УДК 519.688

ЭВРИСТИЧЕСКАЯ ДЕКОМПОЗИЦИЯ ЗАДАЧИ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СИСТЕМАМИ НА ОСНОВЕ МЕТОДА СИТУАЦИОННОГО УПРАВЛЕНИЯ

Ковалев Илья Гаврилович[1], Потемкин Эдуард Константинович[2],
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков, д 22, к.1,
[2] ОАО «ВНИИТрансмаш»,
Россия, Санкт-Петербург, ул. Заречная, д. 2,
e-mail: mail.kovalev@gmail.com.

Аннотация: Предлагается подход к формализации задачи управления системами связи, в том числе специального назначения, с целью повышении эффективности системы управления связью в условиях динамически меняющейся обстановки при взаимодействии разнородных прикладных процессов.

Ключевые слова: *алгоритм классификации; ситуационное управление; телекоммуникационная система; декомпозиция задачи управления.*

HEURISTIC DECOMPOSITION OF THE PROBLEM OF MANAGEMENT OF TELECOMMUNICATION SYSTEMS ON THE BASIS OF SITUATIONAL MANAGEMENT

Kovalev Ilya[1], Potemkin Eduard [2],
[1] The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov, 22-1,
[2] Russia, St. Petersburg, Zarechnaya, 2,
e-mail: mail.kovalev@gmail.com.

Abstract: A proposed approach to formalization of management systems of communication, including special purpose, with the aim of increasing the effectiveness of control system of communication in the conditions of the dynamically changing situation in the interaction of heterogeneous application processes..

Keywords: *the classification algorithm, situational management; telecommunication syste; decomposition management tasks.*

Введение. Процессы конвергенции в системах связи, в том числе специального назначения, происходящие практически на всех уровнях рассмотрения - от унификации технологического взаимодействия до размытия границ бизнеса традиционных операторов связи, создают спрос на комплексные решения по управлению телекоммуникационными системами (ТКС). В настоящее время проектирование АСУ осуществляется вне комплексной модели управления и чаще всего представляет собой эклектичное объединение методов и подходов. Большая часть применяемых методов рассматривает лишь очень частный аспект функционирования ТКС, ограничивая постановку задачи в терминах "малой" модели. Объединение подобных систем осуществляется, как правило, лишь на технологических основах (вне обобщенной постановки задачи управления) и потенциально может привести к потери управляемости системы, представляя угрозу ее существованию.

Постановка задачи. Для характеристики феномена управления используют различные, зачастую пересекающиеся классификаторы [1], требующие, как правило, уточнения в прикладных областях. В настоящей работе предлагается использовать следующие классификационные признаки процесса управления в телекоммуникационных системах:

– по классу модели: «малые» системы (управление «в малом»), «большие»/«сложные» системы (управление «в большом»);

– по типу управления: стратегическое, оперативное, оперативно-техническое, технологическое;

– по административному признаку: международные рекомендации, отраслевые стандарты, корпоративные стандарты, государственные нормативные и правовые акты;

– по информационной модели (трактовке управления): TMN, ISO/OSI, eTOM.

Телекоммуникационная система может быть представлена в каждом из перечисленных аспектов и иметь соответствующую конкретному представлению постановку задачи управления. Актуальной задачей представляется непротиворечивое объединение перечисленных представлений в рамках одной методологии и постановка обобщенной задачи управления телекоммуникационными системами.

Анализ применяемых методов. Вопрос управления ТКС эволюционировал в соответствии с рассматриваемыми концепциями от ISO/OSI к TMN и далее к eTOM. В настоящий момент наиболее актуальным подходом к управлению через построение АСУ является методология NGOSS,

объединяющая все предыдущие концепции на основе набора моделей и процесса реализации (соответственно структур и методологии поддержки в терминологии NGOSS). Тем не менее, управление в той или иной мере проявлено в каждой из этих концепций.

Более подробное их рассмотрение и анализ позволяет сконцентрировать внимание на методологических аспектах управления (см. таблицу 1).

Таблица 1

Методологические аспекты управления в базовых концепциях управления ТКС

Базовые концепции управления ТКС	Ориентация на тип управления и класс АСУ	Предмет	Доминирующий феномен	Класс модели управления	Декомпозиция в задаче управления
TMN	Любой, OSS	Модель ТКС в различных интерпретациях (по уровням TMN)	Процесс взаимодействия управляющего (менеджер) и управляемого (агент) объекта	Малая модель, ОУ отделен от УО	Структурная, функциональная
ISO/OSI	Технологическое OSS	Взаимодействие открытых систем	Процесс взаимодействия открытых систем	Малая модель, управление состоянием	Функциональная
eTOM	Оперативное, оперативно-техническое; OSS/BSS, ERP	Операционная деятельность компании-оператора связи	Операционный процесс	Малая модель, управление состоянием или по эффективности (BSC, KPI и т.д.)	Структурная, функциональная
ФЗ №126	Любой, любая.	Организационно-правовые отношения операторов связи	Система – хозяйствующий субъект	—	Структурная (по организационным, территориальным и т. д. признакам

Анализ таблицы позволяет сделать следующие выводы:

– доминирующим феноменом при описании ТКС является процесс;

– существует противоречие между классом рассматриваемой системы (сложная система) и классом применяемых моделей (малые модели);

– определяется дифференциация процессов на «высокого» и «низкого» уровней, которые поддерживают соответственно системы BSS и OSS, при этом точкой сопряжения является модель eTOM, осуществляющая структурно-функциональную декомпозицию «высоких» процессов к «низким»;

– отсутствует механизм согласования прикладных процессов, АСУ представляется набором средств для автоматизации операционной деятельности, но не решает своей прямой задачи (управления);

– отсутствуют в явном виде средства оценки функционирования системы и реализации многомодельности: рассмотрение процесса как основного феномена проводится в терминах малой системы, что фиксирует интерпретацию системы, а механизма координации процессов, манипулирующих различными интерпретациями системы, отсутствуют;

– исходной позицией является модель системы (eTOM), а не процесс управления.

Обозначенные выводы можно обобщить следующей формулировкой основной проблемы - отсутствие единообразного подхода к формулировке задачи управления, так как каждая из имеющихся концепций рассматривает управление с точки зрения «малой» модели.

Предложения. Согласно полученным выводам, управление телекоммуникационной системой можно представить как отображение прикладных процессов управления на процессы, протекающие на физическом ресурсе (рисунок 1). При этом АСУ рассматривается как «черный ящик», на входе которого (P) - обращения прикладных процессов (заявки), на выходе (R) - процессы на физическом ресурсе, а отображение входа на выход (φ_y) интерпретируется как реализация на ресурсе команд конкретного прикладного процесса.

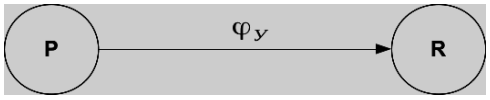


Рис. 1. Обобщенная задача управления телекоммуникационной системой

Задача в такой постановке не имеет конструктивного решения - прямое отображение невозможно:

– представленные объекты P и R могут быть рассмотрены в одном классе моделей, ведь элементами обоих являются процессы, хотя, согласно [2], они являются разными метаязыками;

– анализ использования процессных моделей, в частности, eTOM, не позволяет построить конструктивных процедур взаимодействия прикладных процессов в терминах моделей вход-выход;

– существование функционального отображения между P и R означало бы, в конечном итоге, попытку создания единой модели вход-выход, что противоречит свойствам большой системы.

Классическим случаем, иллюстрирующим актуальность конструктивного разрешения указанных противоречий, является задача оперативно-технического управления при ликвидации последствий ЧС (рисунок 2).

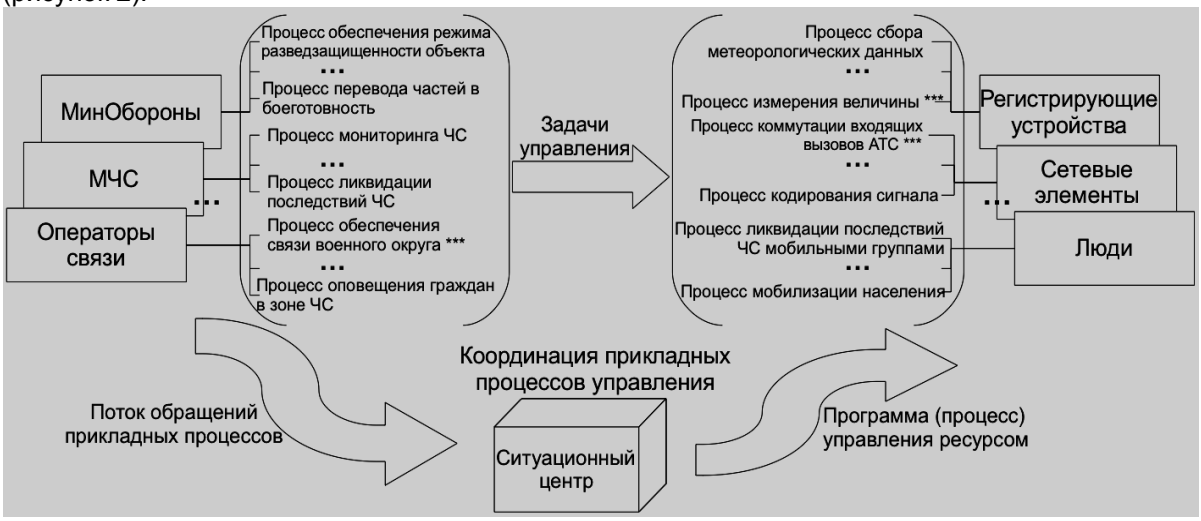


Рис. 2. Интерпретация АСУ в обобщенной задаче управления процессами на примере ситуационного центра управления ЧС

АСУ в данном примере реализована в виде ситуационного центра по управлению системой связи в условиях ЧС; множество должностных лиц и организаций, представленных прикладными процессами, осуществляют воздействие на факторы ЧС используя некий общий ресурс - людей, технику, информацию, так же учитываемые как факторы ЧС. При этом каждый прикладной процесс имеет собственную интерпретацию системы и осуществляет управление в собственных терминах, удовлетворяя собственным критериям [4],[5].

Основная задача, очевидно, состоит в координации действий субъектов (их прикладных процессов) сообразно сложившейся обстановке, что и должен обеспечивать СЦ. Конечно, в условиях дефицита времени и ресурсов, характерных для развития ЧС, построить или настроить АСУ в методологии NGOSS представляется невозможным.

Подобные задачи, хотя и с менее жесткими условиями могут возникать и в обычной деятельности оператора, когда требуется управлять множеством разнородных прикладных процессов (выпуск нового продукта, развитие сети и т. д.).

Приведенный пример ситуационного центра не случаен, именно методология ситуационного управления [1], позволяющая учитывать множественность описания системы, наличие многих, трудно формализуемых и даже антогонистичных целей существования системы, разрабатывалась и успешно применялась для управления сложными системами.

Ключевым понятием метода является ситуация, которое в данной статье будем рассматривать в «классической» трактовке, данной Д.А. Поспеловым в [3]. Ситуация не задается непосредственно ни на множестве прикладных процессов, ни на множестве ресурсов. Являясь внешней, относительно множества прикладных процессов, и множества ресурсов (не описываясь терминами соответствующих моделей), именно ситуация должна обеспечить механизм управления взаимодействием множества прикладных процессов, который позволит избежать «проклятия размерности», связанного с декомпозицией прикладных процессов и определением правил их взаимодействия.

Основные результаты. Для решения поставленной задачи применим известный кибернетический прием - принцип внешнего дополнения [2]. Для этого введем новый объект (ситуацию) и соединим его с объектами и соответственно отображениями, как показано на рисунке 3.

Рассматривая полученную на рисунке 3 тройку как кибернетическую модель, расширяющую исходную задачу управления, где объекты P и R выступают в ролях управляющего и управляемого объекта соответственно, объект Z является «устройством», компенсирующим недостатки формальной модели (P) для корректного управления физическим ресурсом (R).

Так, недостатки формализации eTOM (и, вероятно, любой другой процессной модели), главными из которых являются отсутствие правил взаимодействия и неконструктивность сквозного (до уровня управляющих сигналов в схемах сетевых элементов) описания операционных процессов, должны быть обеспечены этим новым элементом и процедурами py и gy.

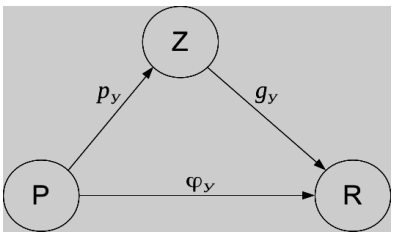


Рис. 3. Применение принципа внешнего дополнения к задаче управления ТКС

Построение этих процедур «как есть» представляется задачей если и разрешимой, то крайне трудоемкой, так как требует учета, в частности, следующих аспектов:

– определение метрики на множестве прикладных процессов, позволяющей определить порядок взаимодействия между процессами, что само по себе является нетривиальной задачей;

– полезностной интерпретации прикладного процесса, которая в eTOM отсутствует и может появиться только на уровне данных (SID), что уже является другим ракурсом системы;

– объект *Z* должен обладать всей информацией обо всех параметрах физического ресурса, что абсурдно для любой сложной системы.

Таким образом, целесообразно продолжить декомпозицию имеющихся процедур. Снова используем принцип внешнего дополнения: определим объекты *L* - множество интерпретаций системы связи, *M* - множество критериев (целей) управления. Будем считать процедуры h_p и h_R осуществимыми по построению в связи со следующим:

– любой процесс имеет операционные характеристики и полезностную интерпретацию, то есть обладает значимостью для ЛПР и связан с оценкой выполнения системой своих функций. Таким образом, операционные процессы могут быть сравнены с точки зрения эффективности, если они обладают полезностной интерпретацией;

– физический ресурс имеет объектное представление как минимум в соответствии с требованиями стандартов построения открытых систем [6]. Наличие указанных стандартов позволяет использовать принципы ООП при моделировании классов единиц физического ресурса в зависимости от используемой интерпретации системы.

Дополним полученную конструкцию до коммутативной диаграммы, добавив процедуры $p_{пр}$ и $g_{пр}$ (см. рисунок 4).

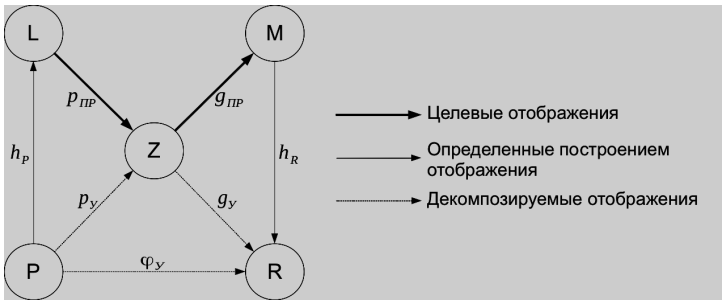


Рис. 4. Эвристическая декомпозиции задачи управления ТКС

Полученная коммутативная диаграмма позволяет выразить исходную задачу отображения прикладных процессов на физический ресурс через последовательность процедур реализующих распределенный процесс принятия решений (см. рисунок 5).

На основе полученных построений можно дать оценку роли ситуации в задаче управления как механизма определения стратегий управления.

Обычно ситуация интерпретируется как множество состояний объекта управления и фиксируется на языке rx-кодов, имея описание текущей ситуации и желаемой строится путь, состоящий из модификаций описания текущей ситуации в желаемую, которым соответствуют элементарные решения по управлению [3].

Подобный подход связан с существенными затратами на построение подобной модели объекта управления и комбинаторной сложностью при поиске лучшего в некотором смысле пути. В предложенной же модели экономичность представления ситуации определяется наличием структуры в объекте.

Таким образом, базовым множеством для определения ситуации в задаче управлении ТКС является множество интерпретаций ТКС, а задача управления ТКС по ситуации может быть сформулирована как определение стратегий управления согласно выбранной интерпретации ТКС.

Формализацию предложенной декомпозиции удобно привести в терминах теории категорий, абстрагируясь от внутреннего устройства элементов диаграммы.

Определим категорию управления:

1) $Ob\ K = \{P, R, L, M, Z\}$

2) $Mor(P, L) = h_P$, $Mor(M, R) = h_R$, $Mor(P, R) = \varphi_У$, $Mor(P, Z) = p_У$, $Mor(Z, R) = g_У$, $Mor(L, Z) = p_{ПР}$, $Mor(Z, M) = g_{ПР}$

3) $\varphi_У = g_У \circ p_У$, $p_У = h_{ПР} \circ h_P$, $g_У = h_R \circ g_{ПР}$, $\varphi_{ПР} = g_{ПР} \circ p_{ПР}$, $\varphi_У = h_R \circ g_{ПР} \circ p_{ПР} \circ h_P$

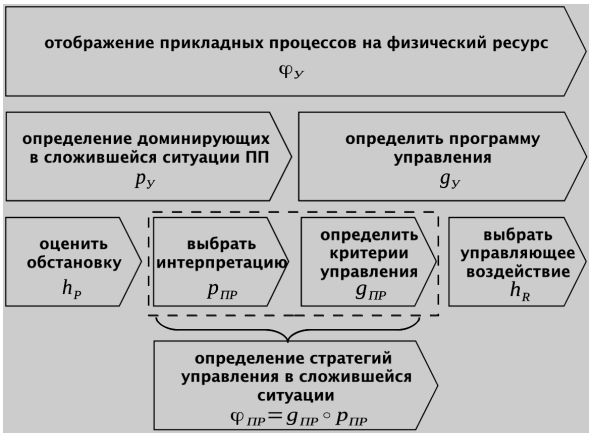


Рис. 5. Эвристическая декомпозиция задачи управления как процесс принятия решений

Представляя объект P как источник требований единственного субъекта управления, задача управления φ_y сводится к задаче принятия решения по выбору управляющего воздействия на физический ресурс из множества управлений, определенных должностными полномочиями субъекта управления, допустимых манипуляций над физическим ресурсом и множеством возможных действий регламентированных операционными процессами субъекта управления. Для случая всей системы, представляемой обращениями многих прикладных процессов, задача управления, так же, может быть сведена к задаче принятия решений, но по выделению ресурса АСУ для удовлетворения требований прикладных процессов, на основе стратегий управления, целесообразных в данной ситуации.

Выводы. Проведенный в работе критический анализ концепций в области управления ТКС позволил сформировать предложения по интерпретации АСУ ТКС в классе больших систем на основе базовых понятий метода ситуационного управления. Полученная в результате проведенного анализа интерпретация задачи управления потребовала дальнейшей декомпозиции, в результате чего была получена эвристическая модель ситуационного управления ТКС, позволяющая:

– учесть комплексность ситуационного управления и множественность интерпретаций ТКС;

– предъявить требования к объекту и определить конструктивные процедуры построения описания ситуации при фиксации модели интерпретации ТКС (переход к конкретной категории).

СПИСОК ЛИТЕРАТУРЫ

1. Волкова, В.Н. Теория систем и системный анализ в управлении организациями: Справочник: Учеб. Пособие/Под ред. В.Н. Волковой и А.А. Емельянова. — М.: Финансы и статистика, 2006. — 848 с.
2. Бир, С. Мозг фирмы: Пер. с англ. / С. Бир. — М.: Радио и связь, 1993. — 416 с.
3. Поспелов, Д.А. Ситуационное управление: теория и практика /Д.А. Поспелов. – М.: Наука, 1986. — 288 с.
4. Райли Дж. NGOSS: Построение эффективных систем поддержки и эксплуатации сетей для оператора связи /Дж. Райли, М. Кринер: Пер. с англ. — М.: Альпина Бизнес Букс, 2007. — 192с.
5. Колбанев М.О., Татарникова Т.М., Малков К.О. Подход к организации адаптивного согласующего центра корпоративной сети Информационно-управляющие системы, № 3, 2008. С. 28-31.
6. ITU-T Recommendations X.200 (07/94)

УДК 621.391.28
ББК 32.811.4

ПРЕДОСТАВЛЕНИЕ СЕРВИСОВ БЕЗОПАСНОСТИ В ПАКЕТНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ В ТЕРМИНАХ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ

Мошак Николай Николаевич, Иванов Виктор Иванович,
ОАО «Интелтех»,
Россия, Санкт-Петербург, ул. Кантемировская, д. 8,
e-mail: nnmoshak49@male.ru.

Аннотация: В статье приводится принципы реализации сервисов безопасности в пакетных мультисервисных сетях связи в терминах открытых систем

Ключевые слова: *сервисы безопасности; мультисервисная сеть связи; модель взаимодействия открытых систем*

SERVICES SECURITY IN MULTI SERVICES COMMUNICATIONS NEWORK IN TERMINUS OF MODEL OPEN SYSTEMS INTERCONNECTED

Moshak Nikolai Nikolaevich, Ivanov Viktor Ivanovich,
PJSC «Intelteh»,
Russia, Saint-Petersburg, Kantemirovskaya str. 8,
e-mail: nnmoshak49@male.ru.

Abstract: Principles realization of security services systems in multiservice communications networks in terminus of model open system interconnected are proposed.

Keywords: *security services; multiservice communications network; open system interconnected model*

В связи с использованием глобальных и региональных мультисервисных сетей связи (МСС) для передачи деловой и конфиденциальной информации введение услуг безопасности в процессе передачи по открытым каналам связи приобретает все более актуальное значение.

Принцип функционально–структурной целостности МСС предписывает моделировать процессы ее функционирования с учетом их совокупности, взаимосвязи друг с другом и сетевым окружением, а также целеполагания системы, т. е. предписывает строить модели функционирования сети с позиций системного подхода [1].

Наиболее естественной основой такого подхода при построении моделей процессов функционирования МСС является концепция моделей сетевых архитектур. Архитектура сети описывает ее внутреннее строение, алгоритмы работы, структуру и состав процедур доступа, обмена и управления, а также построение и взаимосвязь ее логической, программной и физической структур.

Для выявления специфики предоставления сервисов безопасности в МСС воспользуемся языком и принципами формализованного описания объектов исследования, примененные в Базовой эталонной модели Международной организации стандартов (МОС), на основе которой строится модель взаимодействия открытых систем (ВОС), получившая дальнейшее развитие в для моделей архитектур МСС [2].

Систему, удовлетворяющую требованиям стандартов МОС, именуют открытой. Каждая система в модели ВОС рассматривается в виде логически взаимосвязанной совокупности подсистем, образованных в результате пересечения системы с некоторым h–уровнем, который образуют подсистемы одного ранга.

Каждая подсистема состоит из одного или нескольких h–уровневых объектов. Суть уровневой организации – предоставление более высокому смежному логическому уровню сервиса более низкого логического уровня. Сервис безопасности состоит из услуг безопасности.

Стандарт ГОСТ Р ИСО 7498–2–99 определяет пять базовых услуг для обеспечения безопасности (защиты) компьютерных систем и сетей: конфиденциальность (Confidentiality), аутентификация (Authentication), целостность (Integrity), контроль доступа (Access Control), причастность (Nonrepudiation), входящие в архитектуру защиты ЭМ, и механизмы, обеспечивающие функционирование этих услуг.

Услуга безопасности – это функциональные возможности h–уровня, которые предоставляются в распоряжение (h+1)–объектам в h–точках доступа к сервисам (СТД) h-уровня, которые играют роль логических интерфейсов (правил взаимодействия между смежными уровнями) между h-объектами и (h+1)-объектами двух смежных уровней [3].

Точка доступа к сервису – это точка, через которую запрашивается и предоставляется сервис уровня. Каждая точка доступа к сервису имеет индивидуальный адрес, который однозначно идентифицирует конкретный объект (h+1)-уровня, использующий сервис h-уровня, т.е. местоположение h-СТД определяется h –адресом (рисунок 1).

Между (h+1)-объектами, h-объектами и h-СТД существуют определенные соотношения.

Во-первых, объекты, имеющие общую СТД, находятся в одной системе.

Во-вторых, (h+1)-объект может быть подключен к нескольким h-СТД, соединенным с одними и теми же несколькими h-объектами. Однако в каждый момент каждая N-СТД соединена только с одним N-объектом и только с одним (h+1)-объектом, т. к. h-СТД является «входом» в определенный h- и (h+1)-объект и связана поэтому с идентификацией (адресацией) объектов.

В общем случае один адрес может идентифицировать несколько СТД.

В иерархической системе модели ВОС доступ к объекту h-уровня обеспечивается использованием адресов на более низких уровнях.

Интерпретация соответствия между h-адресами, обслуживаемыми h-объектом, и (h-1)-адресами, используемыми для доступа к (h-1)-услугам безопасности, осуществляется с помощью

функции отображения h-адресов. Внутри уровня могут существовать два различных вида функций отображения h-адресов: иерархическое и отображение с помощью таблиц.

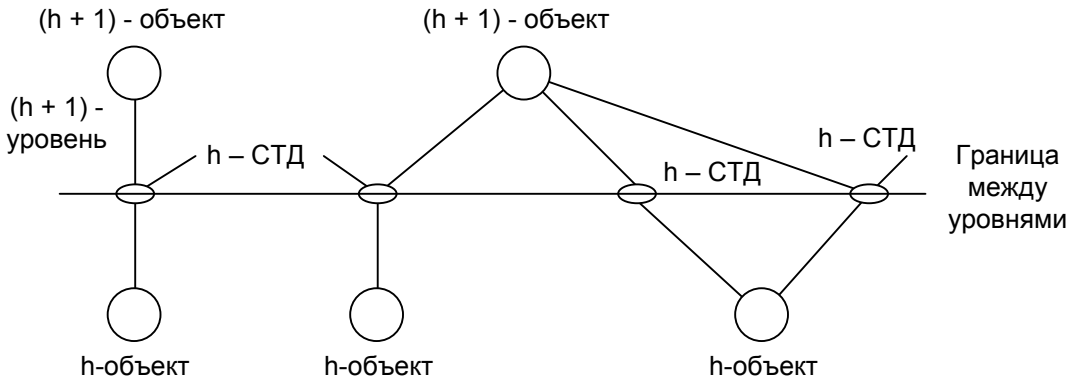


Рис.1. Схема предоставления услуги безопасности h–уровня в h-СТД

Одноранговые объекты h–уровня взаимодействуют между собой с помощью одного или нескольких протоколов через логические соединения, создаваемые на (h–1)–уровне. Спецификация протоколов h–уровня определяет процедуры выполнения сервисов, форматы управляющих и информационных полей протокольных блоков уровня (сервисных примитивов уровня), процедуры обмена протокольными блоками между объектами h–уровня в разных открытых системах, а также механизм выбора указанных процедур из списка возможных. Сервисные примитивы - это концептуальные понятия, облегчающие описание последовательности событий при доступе к сервису уровня и представляют первичные, неделимые элементы описания сервиса. Каждый сервисный примитив является именованной (т. е. имеющей уникальное название) совокупностью параметров.

Концепция сервиса, предоставляемого уровнем, является одной из основных в модели ВОС. Сервис уровня определяется через элементы абстрактной модели взаимодействия пользователей сервиса и поставщика сервиса. Эта модель включает в себя следующие понятия (рисунок 2): пользователи N-сервиса, поставщик N-сервиса и сервисные примитивы. Последние разделяются на примитивы: запроса (request), индикации (indication), ответа (response) и подтверждения (confirmation).

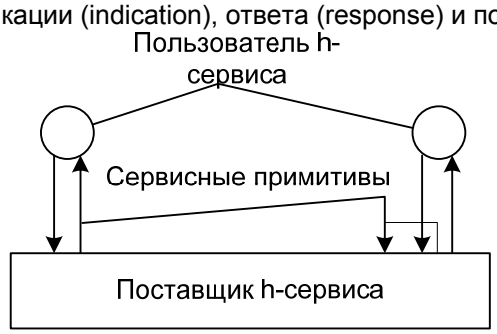


Рис.2. модели взаимодействия пользователей сервиса и поставщика сервиса

Услуги безопасности представляют собой абстрактные понятия, которые характеризуют требования безопасности и могут быть реализованы на одном и/или нескольких логических уровнях архитектуры сети. Услуги безопасности могут быть обязательными и факультативными, а также подтвержденными и неподтвержденными. Обязательность услуги означает, что она должна предоставляться во всех реализациях. Факультативные услуги могут предоставляться или нет в зависимости от назначения реализации. Если сервис безопасности определяется в качестве факультативно предусматриваемой отдельным уровнем, это означает, что он реализуется определенными механизмами защиты, работающими в рамках этого уровня, если иное не оговорено. При этом механизм защиты может включаться в процесс обслуживания протокольного блока уровня для каждого типа информации и/или представлять собой отдельную услугу уровня.

Подтверждаемые услуги - это те, предоставление которых связано с обменом парой сервисных примитивов - примитивом запроса и примитивом подтверждения. Для некоторых неподтверждаемых услуг обмен сервисными примитивами отсутствует - здесь достаточно только передачи запроса от пользователя сервиса. Изложенные понятия являются основой формализованного описания сервиса. Элементы такого описания в настоящее время стандартизованы МОС и называются соглашениями по сервису.

Для реализации базовых услуг безопасности в сети могут применяться как специальные механизмы защиты («Шифрование», «Заполнение трафика», «Управление маршрутизацией», «Цифровая подпись», «Контроль доступа», «Обеспечение целостности», «Аутентификация», «Нотаризация»), так и общие механизмы защиты («Доверительная функциональность», «Метки

безопасности», «Аудиторская проверка»), которые могут быть задействованы для усиления последних. На практике услуги безопасности должны быть включены в соответствующие уровни логической структуры сети для обеспечения требований ее политики информационной безопасности [2]. При этом практическая реализация требований политики может потребовать различных сочетаний базовых услуг защиты в соответствии с их приоритетами с учетом дифференциации по классу трафика.

Опишем процесс вызова услуги безопасности для защиты сеанса связи с установлением мультимедийного соединения в MCC NGN, которая запрашиваются во время его установления. При каждом запросе h–сервиса безопасности (h+1)–объект может запросить желаемую цель защиты.

В запросе указывается конкретная услуга защиты, необходимые параметры услуги и, при необходимости, любая дополнительная релевантная информация (например, о грифе конфиденциальности и/или метка безопасности) в соответствии с целью защиты. Запрос h–услуги безопасности, который формирует (h+1) логический объект, определяет тип и параметры защиты и осуществляется через обращение к информационной базе административного управления защитой (ИБАУЗ).

Перед установлением соединения h-уровень инициирует доступ к ИБАУЗ, которая содержит информацию об административно устанавливаемых требованиях к защите, связанных с (h+1)-объектом. При этом могут передаваться функциональные возможности h-уровня. Передаваемые функциональные возможности призваны усилить административно устанавливаемые требования к защите.

Обеспечение особенностей защиты в течение момента передачи, ориентированной на установление соединения, может потребовать обсуждения условий требуемых служб защиты. h-уровень может отвергнуть запрос службы, если он нарушает административно навязанные требования, записанные в ИБАУЗ для (h+I)-объекта. h-уровень также, должен придать запрашиваемым службам защиты любые службы защиты, определенные в ИБАУЗ в качестве мандатов на получение цели защиты. Если (h+1)-объект не определяет цель защиты, h-уровень должен следовать стратегии защиты в соответствии с ИБАУЗ. Параметры защиты могут устанавливаться по умолчанию.

После определения сочетания административно устанавливаемых и динамически отобранных требований к защите h-уровень должен попытаться достигнуть, как минимум, защиты цели. Это должно достигаться одним или двумя следующими методами: а) непосредственным вызовом механизмов защиты в рамках h–уровня; б) и/или запросом сервисов безопасности на (h–1)–уровне. В этом случае область применения защиты должна быть расширена на h–службу путем сочетания передоверяемых функциональных возможностей и/или специальных механизмов защиты на h–уровне. Таким образом, h–уровень определяет, способен ли он обеспечить требуемую защиту цели, если нет, соединение блокируется.

Обсудим планирование служб в рамках h-уровня (в противоположность передаче нижележащим (h-I)-службам) [4]. В некоторых протоколах для обеспечения удовлетворительной защиты цели последовательность операций является решающей.

а) Опережающий контроль доступа

h-уровень может требовать опережающего контроля доступа, то есть он может локально определять (от информационной базы управления защитой), может ли быть разрешено или запрещено защищенное h-соединение.

б) Аутентификация равноправных объектов

Эта услуга, когда она предусмотрена h-уровнем, предназначена для выдачи подтверждения (N+I)-объекту, что источником данных является равноправный (h+I)-объект.

Если защита цели включает идентификацию равноправных объектов или если известно (из информационной базы управления безопасностью), что назначение h-объекта потребует идентификации равноправного объекта, то должен произойти идентификационный обмен. Для этого может использоваться двух- или трехкртное квитирование установления связи для обеспечения односторонней или взаимной идентификации. Идентификационный обмен может быть объединен либо с обычными процедурами установления h-соединения, либо осуществлен отдельно от установления h-соединения.

в) Контроль доступа

Назначение h-объекта или промежуточных объектов может потребовать ограничений контроля доступа. Если специфическая информация затребована через механизм дистанционного контроля доступа, то h-объект, являющиеся инициатором, предоставляет эту информацию в рамках протокола (N)-уровня или через каналы управления.

г) Конфиденциальность

Если была выбрана служба полной или избирательной конфиденциальности, то должно быть установлено защищенное h-соединение. Это может включать установление собственных рабочих ключей и обсуждение криптографических параметров соединения. Это может быть сделано путем предварительной компоновки в идентификационном обмене или путем отдельного протокола.

д) Целостность данных

Эта служба, когда она предусмотрена h-уровнем, предназначена для выдачи подтверждения (N+I)-объекту, что источником данных является заявленный равноправный (h+I)-объект.

Если была выбрана целостность данных всех h-пользователей с восстановлением или без восстановления или целостность отдельных полей протокольного блока данных, то необходимо установить защищенное h-соединение.

Оно может быть аналогично соединению с задействованием службы конфиденциальности, и может предусматривать идентификацию. К защищенному h-соединению применимы те же соображения, что и для службы конфиденциальности.

е) Службы безотказности

Если была выбрана безотказность с подтверждением происхождения, необходимо установить собственные криптографические параметры или же установить защищенное соединение с объектом, осуществляющим нотаризацию. Если была выбрана безотказность с подтверждением доставки, необходимо установить собственные параметры (которые отличаются от параметров, требуемых для безотказности с подтверждением происхождения) или установить защищенное соединение с объектом, осуществляющим нотаризацию.

В сеансе связи в процессе передачи данных по защищенному h-соединению должны быть задействованы конкретные службы защиты. В рамках h-службы должно быть организовано:

а) идентификация равноправных объектов (в интервалах);

б) защита выбранных полей;

в) сигнализация об активных нападениях (например, службой «целостность соединения без восстановления» при возникновении манипуляций данными. Кроме того, может потребоваться запись ревизии следа защиты, обнаружение события и управление событием.

Механизмы защиты могут быть реализованы как в виде отдельных процедур, так и являться неотъемлемой частью протоколов установления соединения.

Механизмы защиты, реализующие услуги безопасности в рамках связных протоколов, моделируются системами массового обслуживания с протокольной услугой безопасности, а в рамках отдельных процедур – системами массового обслуживания с самостоятельной услугой безопасности [1,5].

Последние, в том числе включают в себя формализацию процессов управления безопасностью и могут включать как фазы формирования и передачи сервисных примитивов трафика безопасности на дополнительном логическом уровне архитектуры сети, так и фазу их обработки в конечных и/или промежуточных системах с учетом QoS-норм передачи основных информационных потоков.

В любом случае, реализация механизмов защиты осуществляется по принципам предоставления сервиса ВОС [2], при этом механизмы защиты в различных сочетаниях могут быть реализованы на различных уровнях архитектуры МСС [1].

СПИСОК ЛИТЕРАТУРЫ

1. Н. Н. Мошак. Защищенные инфотелекоммуникации. Анализ и синтез: монография / СПб.: ГУАП, 2014. 193 с.: ил.
2. ISO/IS 8509. Information Processing Systems. Open System Interconnection. Basic Reference Model.
3. Зайцев С.С. Кравцунов М.И., Ротанов С.В. Сервис открытых информационно-вычислительных сетей: справочник. М.: Радио и связь. 1990. 240 с.: ил.
4. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. – М., ИПК Издательство стандартов, 1999
5. Мошак Н.Н. Формализация и оценка процессов представления механизмов защиты в мультисервисной сети. Общий подход // «Электросвязь», №3, 2012.

УДК 004.056.5

РАСПРЕДЕЛЕНИЕ СИЛ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ДИНАМИЧЕСКОЙ СРЕДЫ ИНФОРМАЦИОННЫХ УГРОЗ

Левкин Игорь Михайлович[1], Галкова Елена Александровна[2],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, д. 49,
e-mail: lev.kin@mail.ru.

Аннотация: Рассматривается задача оптимального распределения сил и средств защиты информации по узлам информационной структуры предприятия в условиях изменения потока и направленности информационных угроз, характерного при осуществлении комплексных деструктивных воздействий.

Ключевые слова: *информационная угроза; нарушитель; деструктивные воздействия; актив предприятия; комплексная защита; оптимальное распределение средств защиты*

THE DISTRIBUTION OF FORCES AND MEANS OF INFORMATION PROTECTION IN THE CONDITIONS OF DYNAMIC ENVIRONMENT INFORMATION THREATS

Levkin Igor [1], Galkova Elena[2],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2]St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverkskiy av. 49,
e-mail: lev.kin@mail.ru.

Abstract: Considered the problem of optimal distribution of forces and means of information protection at the sites of the information structure of the enterprise in the conditions of changing the flow and direction of information threats, characteristic during implementation of the destructive impacts.

Keywords: *information threat; the intruder; destructive impact; active enterprises; comprehensive protection; optimal distribution of protection means.*

Важнейшим элементом безопасности предприятия является информационно-экономическая безопасность. Под информационно-экономической безопасностью защиту жизненно важных интересов предприятия от внутренних и внешних информационных угроз, возникающих в экономической сфере. При этом информационные угрозы экономической безопасности определим как совокупность условий, факторов и событий, которая определяет эффективность деструктивных информационных воздействий на все сферы деятельности предприятия (управленческие, технологические, финансовые и т.п.) [1],[2].

Важнейшими особенностями информационных угроз в современном информационном обществе являются:

– постоянное возникновение новых информационных угроз вследствие обострения информационной борьбы, сбоев в работе внутренних и внешних информационных систем, роста киберпреступности и т.п.;

– наличие системной взаимосвязи большинства информационных угроз, которая выражается в том, что реализация одной информационной угрозы влечет за собой целую совокупность (цепочку) других, связанной с ней информационных угроз;

– приобретение совокупностью информационных угроз динамического характера, проявляющегося в изменении их интенсивности в зависимости от состояния информационно-экономической среды.

В этих условиях существующая система защиты информации предприятия не всегда эффективно справляется с постоянным изменением характера и интенсивности информационных угроз [3]. Это связано: во-первых, с ограниченными возможностями существующих средств защиты информации, ориентированных на предотвращение только ранее известных информационных угроз; во-вторых, с ограниченным, как правило, составом сил и средств защиты информации, имеющемся на каждом предприятии; в-третьих, с отсутствием научно обоснованных подходов, позволяющих оперативно перераспределять силы и средства защиты информации в зависимости от интенсивности и направленности информационных воздействий.

Учет перечисленных особенностей информационных угроз требует разработки новых подходов к организации защиты информации предприятий.

В основу методического аппарата рационального распределения сил и средств защиты информации в условиях динамического характера среды информационных угроз могут быть положены два основных элемента: разработка математических моделей динамической среды угроз информационной безопасности (ДСУ ИБ); формализация задачи динамического распределения сил и средств защиты информации по информационным элементам информационной структуры предприятия и разработка алгоритмов ее решения.

Формализованное описание ДСУ ИБ (в канонической форме) представим в виде многомерного вектора $W_{<x>}$, включающего статистические $W^{c}_{<x'>}$ и динамические $W^{\partial}_{<x''>}$параметры:

$$W_{<x>} =< W^{(1)}_{<\ell_1>},...,W^{(x)}_{<\ell_x>},...,W^{(X)}_{<\ell_X>} > ,$$

$W^{(x)}_{<\ell_x>}$ - ℓ_x-мерный вектор параметров описывающий *x*-параметр ДСУ ИБ; $x=\overline{1,X}$.

$$W_{<x>} = W^{c}_{<x'>} + W^{\partial}_{<x''>}, \qquad x = x' + x''.$$

Каждый параметр вектора $W_{<x>}$ имеет свой информационный аналог, состоящий из одной или нескольких информационных структур (угроз), описываемых информационными признаками (информационно-признаковыми моделями).

К основным статическим параметрам относятся: $W^{c}_{<x'>} = W^{c}_{<6>} = < W^{c(1)}_{<\ell_1>}, W^{c(2)}_{<\ell_2>}, \ldots, W^{c(6)}_{<\ell_6>} >$, где:

1. $W^{c(1)}_{<\ell_1>} = W^{c(1)}_{<4>} < \omega^{c(1)}_1, \omega^{c(1)}_2, \omega^{c(1)}_3, \omega^{c(1)}_4 >$ - характер дестабилизирующего воздействия: $\omega^{c(1)}_1$ – единичная угроза; $\omega^{c(1)}_2$ – множественная угроза; $\omega^{c(1)}_3$ –концентрированное дестабилизирующее воздействие; $\omega^{c(1)}_4$ – дестабилизирующая операция.

2. $W^{c(2)}_{<\ell_2>} = W^{c(2)}_{<10>} < \omega^{c(2)}_1, \omega^{c(2)}_2, \ldots, \omega^{c(2)}_{10} >$ - основные причины возникновения дестабилизирующего воздействия (как внутри объекта, так и вне его):

$\omega^{c(2)}_1$ –случайное единичное внешнее воздействие (заражение вирусом, отключение питания, бросок напряжения и т.п.);

$\omega^{c(2)}_2$ –случайное единичное внутреннее воздействие (отказы и сбои в работе отдельных компьютеров, ошибки в работе их программного обеспечения, ошибки отдельных пользователей и системных администраторов, нарушения отдельными сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации и т.п.);

$\omega^{c(2)}_3$ –случайное групповое внешнее воздействие (заражение разнообразными вирусами ряда компьютеров, приобретение и использование нелицензионного программного обеспечения и т.п.);

$\omega^{c(2)}_4$ –случайное групповое внутреннее воздействие (отказы и сбои в работе ряда компьютеров, ошибки в работе их программного обеспечения, многочисленные ошибки пользователей и системных администраторов, нарушения многими сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации и т.п.);

$\omega^{c(2)}_5$ –целенаправленное враждебное действие бывших сотрудников;

$\omega^{c(2)}_6$ –целенаправленное вредительское действие сотрудников;

$\omega^{c(2)}_7$ –некачественный менеджмент на объекте;

$\omega^{c(2)}_8$ –деятельность конкурентов по получению экономических (финансовых, технологических и т.п.) преимуществ;

$\omega^{c(2)}_9$ – дискредитация объекта;

$\omega^{c(2)}_{10}$ – попытка криминальных структур захватить объект.

3. $W^{c(3)}_{<\ell_3>} = W^{c(3)}_{<7>} = < \omega^{c(3)}_1, \omega^{c(3)}_2, \ldots, \omega^{c(3)}_7 >$ - характер объекта: $\omega^{c(3)}_1$ –государственный деятель; $\omega^{c(3)}_2$ –общественный деятель; $\omega^{c(3)}_3$ – предприятие, имеющее стратегическое значение; $\omega^{c(3)}_4$ – государственное предприятие; $\omega^{c(3)}_5$ –частное предприятие; $\omega^{c(3)}_6$ – общественная организация; $\omega^{c(3)}_7$ – объект муниципальной собственности.

4. $W^{c(4)}_{<\ell_4>} = W^{c(4)}_{<3>} = < \omega^{c(4)}_1, \omega^{c(4)}_2, \omega^{c(4)}_3 >$ - наличие на объекте сил и средств защиты информации: $\omega^{c(4)}_1$ –в достаточном объеме; $\omega^{c(4)}_2$ –в ограниченном объеме; $\omega^{c(4)}_3$ –отсутствуют.

5. $W^{c(5)}_{<\ell_5>} = W^{c(5)}_{<2>} = < \omega^{c(5)}_1, \omega^{c(5)}_2 >$ - правовая база: $\omega^{c(5)}_1$ –развита; $\omega^{c(5)}_2$ –неразвита.

6. $W^{c(6)}_{<l_6>} = W^{c(6)}_{<3>} = < \omega^{c(6)}_1, \omega^{c(6)}_2, \omega^{c(6)}_3 >$ - напряженность внутренней обстановки: $\omega^{c(6)}_1$ – высокая; $\omega^{c(6)}_2$ – средняя; $\omega^{c(6)}_3$ – низкая.

7. $W^{c(7)}_{<l_7>} = W^{c(7)}_{<3>} = < \omega^{c(7)}_1, \omega^{c(7)}_2, \omega^{c(7)}_3 >$ - напряженность внешней обстановки: $\omega^{c(7)}_1$ – высокая; $\omega^{c(7)}_2$ –средняя; $\omega^{c(7)}_3$ – низкая.

К основным динамическим параметрам относятся: $W^{\partial}_{<x''>} = W^{\partial}_{<5>} = < W^{\partial(1)}_{<h_1>}, W^{\partial(2)}_{<h_2>}, \ldots, W^{\partial(5)}_{<h_5>} >$, где:

1. $W^{\partial(1)}_{<h_1>} = W^{\partial(1)}_{<3>} =< \omega^{\partial(1)}_1, \omega^{\partial(1)}_2, \omega^{\partial(1)}_3 >$ - темп развития внутренней угрозы: $\omega^{\partial(1)}_1$ – высокий; $\omega^{\partial(2)}_2$ – средний; $\omega^{\partial(3)}_3$ – низкий.

2. $W^{\partial(2)}_{<h_2>} = W^{\partial(2)}_{<3>} =< \omega^{\partial(2)}_1, \omega^{\partial(2)}_2, \omega^{\partial(2)}_3 >$ - темп развития внешней угрозы: $\omega^{\partial(2)}_1$ – высокий; $\omega^{\partial(2)}_2$ – средний; $\omega^{\partial(2)}_3$ – низкий.

3. $W^{\partial(3)}_{<h_3>} = W^{\partial(3)}_{<3>} =< \omega^{\partial(3)}_1, \omega^{\partial(3)}_2, ..., \omega^{\partial(3)}_7 >$ – этапы (фазы) развития угрозы: $\omega^{\partial(3)}_1$ – зарождение угрозы (принятие решения на формирование угрозы); $\omega^{\partial(3)}_2$ – формирование условий для возникновения угрозы; $\omega^{\partial(3)}_3$ – сбор информации об объекте из открытых источников; $\omega^{\partial(3)}_4$ – проникновение в информационную структуру объекта; $\omega^{\partial(3)}_5$ – использование законных (белых) методов (схем) реализации угрозы; $\omega^{\partial(3)}_6$ – использование серых методов (схем) реализации угрозы; $\omega^{\partial(3)}_7$ – использование черных методов (схем) реализации угрозы.

4. $W^{\partial(4)}_{<h_4>} =< \omega^{\partial(4)}_1, \omega^{\partial(4)}_2, \omega^{\partial(4)}_3 >$ - преследуемые цели: $\omega^{\partial(4)}_1$ – уничтожение объекта; $\omega^{\partial(4)}_2$ – захват объекта; $\omega^{\partial(4)}_3$ – изменение направления деятельности объекта.

5. $W^{\partial(5)}_{<h_5>} = W^{\partial(5)}_{<1>} =< \omega^{\partial(5)}_1, \omega^{\partial(5)}_2, \omega^{\partial(5)}_3, \omega^{\partial(5)}_4 >$ - состав и возможности сил, формирующих угрозу: $\omega^{\partial(5)}_1$ – отдельное лицо; $\omega^{\partial(5)}_2$ – легальная группа лиц; $\omega^{\partial(5)}_3$ – легальная организация; $\omega^{\partial(5)}_4$ – криминальная группировка.

Таким образом, каждая информационная угроза может быть описана совокупностью статических и динамических параметров:

$$W^{y}_{<K>} = W^{y}_{<K>}(\omega^{c(\bullet)}_r, ..., \omega^{\partial(\bullet)}_K)),$$

где $c(\cdot) \in [c(1), c(2), ...c(7)]$, $\partial(\cdot) \in [\partial(1), \partial(2), ..., \partial(5)]$, $r \in [1, 2, 3, ...]$.

На каждый элемент информационной структуры предприятия одновременно или последовательно может воздействовать несколько информационных угроз. Элементами информационной структуры являются: серверы обмена информацией, серверы баз данных, автоматизированные рабочие места сотрудников и руководящего персонала, коммутаторы, линии связи, множительная техника, хранилища документации (сейфы, шкафы и т.п.), другие элементы.

В свою очередь каждый элемент информационной структуры предприятия может быть оснащен несколькими средствами защиты информации. К основным из них относятся [3],[4]:

– программные средства или системы (программы работы с BIOS, программные файерволы, антивирусные средства и т.д.) установленные на рабочей станции и функционирующие в соответствии с выполнением собственных алгоритмов;

– специальные серверы-посредники; системы контроля и управления доступом;

– системы видеонаблюдения, замки, решетки на окнах, защитная сигнализация, устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации и др.;

– генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить; защищенные хранилища носителей информации;

– сертифицированные по требованиям безопасности информации специальных защитных знаков, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;

– специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

– технические средства, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

– резервирование технических средств, дублирование массивов и носителей информации; физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;

– системы аутентификации пользователя при доступе к защищаемой информации, аудита доступа, ведение списка пользователей, блокирование доступа; криптографические средства; физическая охрана; другие средства.

Весь перечень информационных угроз предприятию в процессе его функционирования можно разделить на две группы [2]: постоянно существующие, например, заражение вирусами, типовые утечки информации, действия известных конкурентов по несанкционированному доступу к конфиденциальной информации, утеря документов и т.п.; внезапно возникающие, например, действия сторонних акторов по противодействию нормальной деятельности предприятия в рамках целевых дестабилизирующих действий и информационно-психологических операций, воровство конфиденциальной информации с целью обогащения и т.п.

Возможность появления информационных угроз второй группы предполагает принятие мер по их своевременной идентификации и защите соответствующих информационных узлов.

Решение этой задачи возможно путем динамического перераспределения сил и средств защиты информации по информационным узлам информационной структуры предприятия в зависимости от интенсивности и направленности прогнозируемых новых информационных угроз [5]. При этом предлагается весь комплект сил и средств защиты информации предприятия разбить на две части: базовый комплект, осуществляющий постоянную защиту от стандартных информационных угроз, и маневренный комплект, позволяющий наращивать степень информационной защиты отдельных информационных узлов в зависимости от складывающейся информационно-экономической обстановки.

Структура задачи распределения сил и средств противодействия информационным угрозам на ***i***-м этапе дестабилизирующих воздействий представлена на рисунке 2.

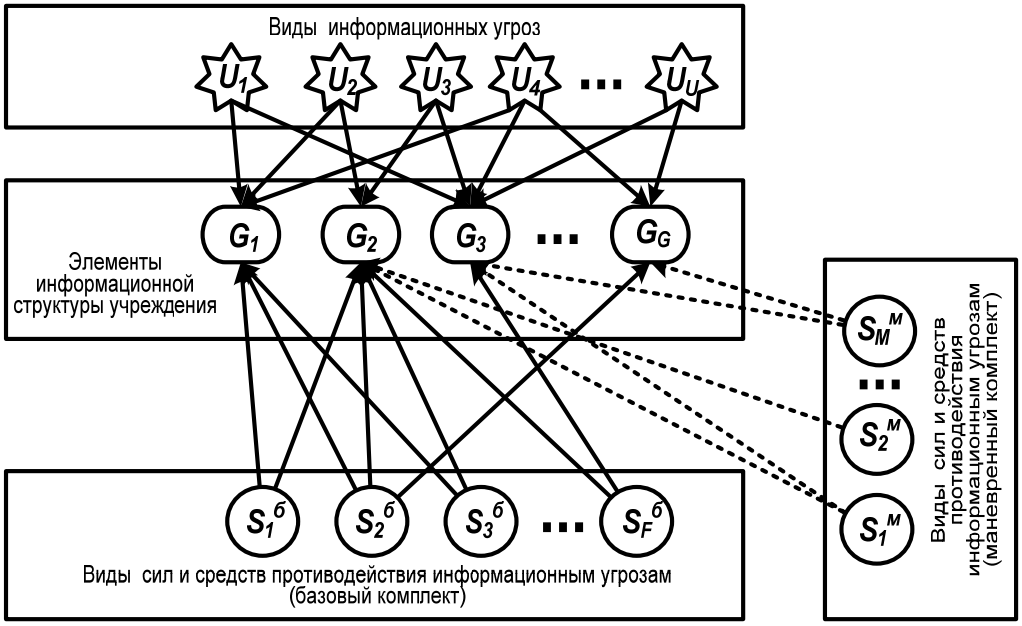


Рис. 2. Структура задачи распределения сил и средств противодействия информационным угрозам на *i*-м этапе дестабилизирующих воздействий

Решение представленной задачи предполагается осуществить в два этапа.

На первом этапе осуществляется распределение базового комплекта сил и средств противодействия информационным угрозам $S_f^б, f=\overline{1,F}$ по информационным узлам информационной структуры учреждения $G_g, g=\overline{1,G},$ $G-$число информационных узлов, подлежащих защите. Это распределение осуществляется путем решения задачи поиска максимума математического ожидания числа решенных задач информационной защиты узлов информационной структуры предприятия Φ^{η}с вероятностью выше заданной P^*_g:

$$\Phi=\frac{1}{G}\sum_g \alpha_g P_g[(\bigcap_i W^{y_i}_{g_{<K>}}((\omega_1^{c_i(\cdot)},...,\omega_K^{\partial_i(\cdot)})),W^з_{g_{<F>}}(S^б_{g_{<F>}})]\xrightarrow[S^б_{g_{<F>}}]{}\max,$$

где $P_g[(\bigcap_i(W^{y_i}_{g_{<K>}}(\omega_1^{c_i(\bullet)},...,\omega_K^{\partial_i(\bullet)})),W^з_{g_{<F>}}(S^б_{g_{<F>}})]-$ вероятность защиты *g*-го информационного узла совокупностью базовых сил и средств защиты информации $W^з_{<F>}(S^б_{g_{<F>}})$ от фиксированной совокупности информационных угроз $\bigcap_i W^{y_i}_{g_{<K>}}(\omega_1^{c_i(\bullet)},...,\omega_K^{\partial_i(\bullet)})$,

α – коэффициент важности g – го информационного узла;

$y \in [c^{(2)}, c^{c(3)}, \partial^{(3)}, \partial^{(4)}, \partial^{(5)}]$;

$K \in [l_2, , l_3, h_3, h_4, h_5]$;

$$\bigcap_i W^{y_i}_{g_{<K>}}(\omega_1^{c_i(\cdot)}, ..., \omega_K^{\partial_i(\cdot)}) = const;$$

$$S^{б}_{g} = < s^{б}_{g_1}, s^{б}_{g_2}, ..., s^{б}_{g_F} >;$$

$$P_g(\cdot) \geq P^*_g;$$

$$\sum_g s^{б}_{g_f} = S^{б}_{f}.$$

На втором этапе осуществляется распределение маневренного комплекта сил и средств противодействия информационным угрозам S^{M}по информационным узлам информационной структуры учреждения на каждом этапе развития комплексной информационной угрозы η.

Это распределение осуществляется путем решения задачи поиска максимума математического ожидания нового числа решенных задач информационной защиты узлов информационной структуры предприятия Φ^{η} с вероятностью выше заданной P^*_g:

$$\Phi^{\eta} = \frac{1}{G}\sum_g \alpha_g P^{\eta}_g [(\bigcap_i W^{y^{\eta}_i}_{g_{<K>}}((\omega_1^{c_i(\bullet)}, ..., \omega_K^{\partial_i(\bullet)})), W^{s^{\eta}}_{g_{<F>}}(S^{б^*}_{g_{<F>}} + S^{м}_{g_{<F>}})] \xrightarrow[S^{м}_{g_{<F>}}]{} \max,$$

$$S^{м}_{g} = < s^{м}_{g_1}, s^{м}_{g_2}, ..., s^{м}_{g_F} >;$$

$S^{б^*}_{g_{<F>}}$ – оптимальное распределение базового комплекта

$$\sum_g s^{м}_{g_f} = S^{м}_{f}.$$

Обе поставленные задачи оптимального распределения сил и средств защиты информации по узлам информационной структуры предприятия могут быть решены известными методами математического программирования, например при использовании пакета MATLAB [6].

Таким образом, использование предлагаемого подхода позволяет осуществить оптимальное динамическое распределение сил и средств защиты информации по узлам информационной структуры предприятия в условиях изменения потока и направленности информационных угроз, характерного при осуществлении комплексных деструктивных воздействий.

СПИСОК ЛИТЕРАТУРЫ

1. Левкин И.М., Левкина С.В., Сорокина Е.А. Информационно-признаковое моделирование угроз национальной безопасности// Вестник Академии военных наук. Северо-Западное отделение, 2013.
2. Левкин И.М., Микадзе С.Ю. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе// VIII Санкт-Петербургская межрегиональную конференцию «Информационная безопасность регионов России (ИБРР-2013)», 2013.
3. Татарникова Т.М. Задача синтеза комплексной системы защиты информации в ГИС//Ученные записки РГГМУ, №30, 2013. С. . С. 204-211.
4. Бескид П.П., Татарникова Т.М. О некоторых подходах к решению проблемы авторского права в сети Интернет//Ученые записки РГГМУ, № 15, 2010. С. 199-210.
5. Попова Е.В. Расчет конкурентоспособности малых предприятий сферы сервиса при усилении информационной безопасности // Вестник российской академии естественных наук,. №16(3), 2012. С. 48–51.
6. Ануфриев И.Е., Смирнов А.Б., Смирнова Е.Н. MATLAB 7. – СПб.: БХВ-Петербург, 2005.

УДК: 621.396.4

СЕТЕВОЙ МОНИТОРИНГ КАК КЛЮЧЕВОЙ ЭТАП ПОДГОТОВКИ И ПРИНЯТИЯ РЕШЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Паращук Игорь Борисович,
Военная академия связи,
Россия, Санкт-Петербург, пр-т Тихорецкий, д. 3,
e-mails: shchuk@rambler.ru.

Аннотация: В статье рассмотрены место и роль мониторинга в рамках задач управления качеством безопасности информации региональных телекоммуникационных сетей. Приведены основные

понятия, используемые при описании пространства состояний принятия решения по безопасности информации.

Ключевые слова: *безопасность информации; телекоммуникационная сеть; мониторинг; цикл управления.*

NETWORKING MONITORING AS THE BASIC OF STAGE PREPARATION AND ADOPTION DECIDE AFTER THE CONTROL OF INFORMATION SECURITY OF REGIONAL TELECOMMUNICATION NETWORKS

Paraschuk Igor,
Military Telecommunication Academy,
Russia, Saint-Petersburg, Tihoretsky str. 3,
e-mail: shchuk@rambler.ru.

Abstract. This article discusses place and role of monitoring in the framework of control problems by quality of information security regional telecommunication network. Furthermore, the main concepts used in description of state space of an adoption decide after the information security are given.

Keywords: *information security; telecommunication network; monitoring; control cycle.*

Введение. Процессы мониторинга состояния и качества информационной безопасности (ИБ) региональных телекоммуникационных сетей (РТКС) являются неотъемлемой частью процесса управления такими сложными системами. Анализ публикуемых данных, посвященных проблемам управления ИБ сложных телекоммуникационных сетей, позволил выделить несколько этапов в цикле управления ИБ сетей такого класса, определить общую роль и место задач мониторинга состояния (качества) ИБ в цикле управления ИБ сети. Основу организации и проведения всех мероприятий по управлению ИБ РТКС, составляют решения должностных лиц (сетевых администраторов), принимаемые в цикле управления ИБ.

Основная часть. Общая технология подготовки (выработки) и принятия решения по управлению ИБ РТКС имеет циклический характер [1], [2] и ярко выраженную иерархическую структуру, которая может быть представлена в виде двух уровней:

1-й уровень, которому соответствует цикл выработки решения, состоящий, в свою очередь, из двух этапов - обоснования и принятия решения;

2-й уровень, которому соответствует цикл генерирования вариантов решений, включающий этап подготовки, собственно поиска (генерирования) и анализа варианта (альтернативы).

Общая технология (организация) процесса управления ИБ РТКС и ее взаимосвязь с технологией подготовки и принятия решения на каждом из этапов реализации данного процесса может быть представлена в виде цепочки мероприятий:

Внутри цикла управления ИБ РТКС - оценка обстановки; выработка замысла (плана); выработка команд управления; подготовка к введению управляющих воздействий; доведение управляющих воздействий до элементов системы ИБ.

Внутри цикла выработки решения два этапа:

Этап обоснования решения (время работы экспертов, системы поддержки принятия решений (СППР)): рассмотрение альтернативных вариантов; акт принятия решения экспертами, СППР [2].

Этап принятия решения (время работы лица, принимающего решение (ЛПР) и акт принятия решения ЛПР).

Внутри цикла выработки варианта – задание варианта решения, решение варианта, анализ варианта решения по управлению ИБ РТКС.

В общем случае, решения в процессе управления структурой, параметрами и режимами работы системы ИБ РТКС, принимаются на всех уровнях иерархии, но применительно ко всему процессу управления, как процессу достижения поставленных целей, решения, принимаемые в ходе (в цикле) оперативно-технического управления ИБ РТКС можно условно разделить на три категории: информационное решение; организационное решение; собственно (окончательное) оперативно-техническое решение.

Таким образом, в соответствии с этими категориями подготовку и принятие решений по организационно-техническому управлению ИБ РТКС можно разбить на три крупных этапа [1]: выработка информационного решения (оценка состояния и качества ИБ РТКС); выработка организационного решения (выработка замысла управления ИБ РТКС) и выработка окончательного оперативно-технического решения (разработка управляющих воздействий, команд управления).

Взаимосвязь основных этапов подготовки и принятия решений по управлению ИБ РТКС представлена на рис. 1.

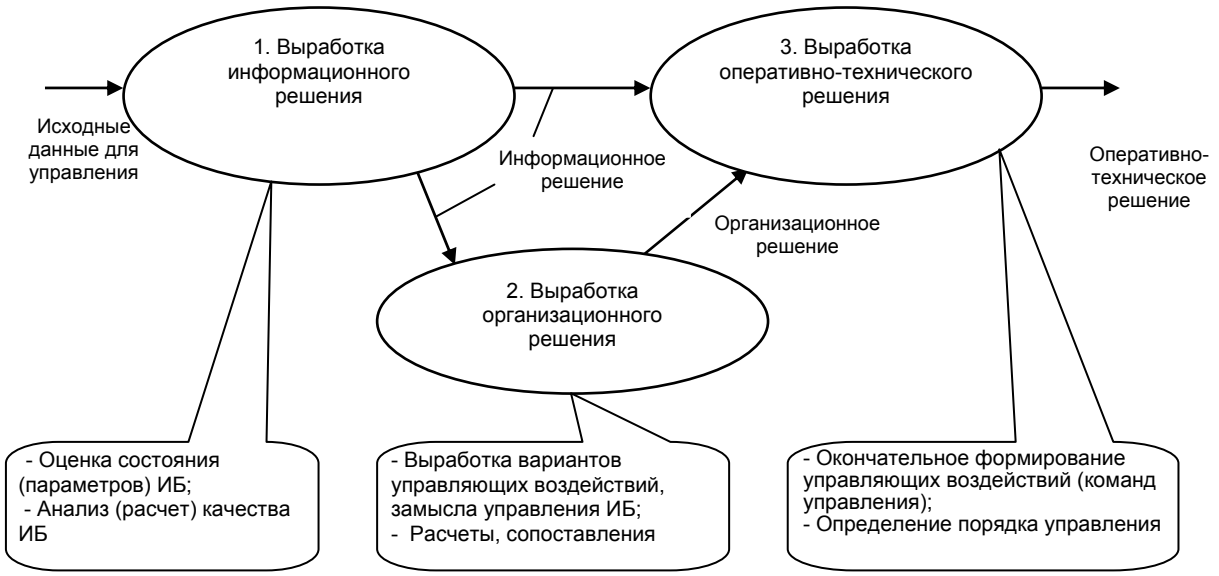


Рис. 1. Этапы подготовки и принятия решений по управлению ИБ

Рассмотрим этапы подготовки, принятия решения по управлению ИБ РТКС и соответствующие им категории решений.

Информационное решение вырабатывается в результате уяснения стоящих перед ИБ РТКС задач, определяемых верхним иерархическим уровнем управления и текущего оценивания состояния ИБ. Данное решение представляет собой результат анализа состояния ИБ РТКС, результат текущей оценки качества объекта ИБ и процесса его функционирования.

Организационное решение соответствует разработке варианта вектора управляющих воздействий и является стержнем оперативно-технического управления ИБ РТКС. На основе полученных новых данных детализируются выводы из информационного решения. Полученные на начальном этапе принятия организационного решения результаты составляют основу замысла управления ИБ РТКС – предположения, детали основного варианта решения поставленной задачи управления ИБ. Именно на этом этапе выделяются основные пути, средства и элементы управления, определяются те основные варианты введения управляющих воздействий, которые на первый взгляд являются целесообразными. Замысел оперативно-технического управления ИБ может включать в себя один или несколько вариантов введения управляющих воздействий. Дальнейший процесс выработки решения по управлению ИБ в том и состоит, чтобы на основе расчетов, сопоставлений и логических рассуждений выбрать тот из них, который в прогнозируемых условиях является наилучшим. Расчеты – один из важнейших элементов принятия решения. Цель расчетов – определить реальность намеченного замысла управления ИБ РТКС, установить, какой из возможных вариантов управляющих воздействий будет наилучшим.

После текущей оценки состояния ИБ РТКС и выработки общей концепции (замысла) управления ИБ РТКС начинается важнейший этап управления, который завершается принятием окончательного оперативно-технического решения. На этом этапе осуществляется окончательное формирование управляющих воздействий (команд управления) и определение порядка управления структурой, параметрами и режимами работы системы ИБ РТКС. Появляется возможность для прогностической оценки состояния ИБ. Разработанный вариант управляющих воздействий утверждается ЛПР, команды управления доводятся до элементов системы ИБ РТКС.

Вся взаимосвязанная совокупность элементов оперативно-технического решения составляет структуру решения по управлению ИБ РТКС.

Заключение. Таким образом, процесс оценки обстановки, включающий сбор и систематизацию информации о состоянии среды функционирования РТКС (с точки рения ИБ), оценивание состояния ИБ РТКС и элементов системы ИБ, является основополагающим, базовым процессом в структуре цикла управления ИБ. Качество оперативно-технического решения по управлению структурой, параметрами и режимами работы системы ИБ РТКС в огромной степени определяется полнотой и рациональностью информационного решения – результатами сетевого мониторинга ИБ РТКС.

СПИСОК ЛИТЕРАТУРЫ

9. Бородакий Ю.В., Курносов В.И., Масановец В.В., Паращук И.Б. и др. Основы теории управления в системах специального назначения: Учебник / под ред. Ю.В. Бородакия. – М.: Управление делами Президента РФ, 2008, 400с.
10. Паращук И.Б., Бабошин В.А., Васильев В.А. Классификация и особенности систем поддержки принятия решений специального назначения // Научно-технический сборник «Телекоммуникационные технологии». Выпуск 8. – СПб.: ГУП НИИ «Рубин», 2012, 148с.

УДК 654.07

УПРАВЛЕНИЕ РИСКАМИ НА РАЗЛИЧНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Салухов Владимир Иванович, [1], Шевченко Олег Игоревич [2],
[1] Россия, Санкт-Петербург, Санкт-Петербургский институт информатики и автоматизации РАН, Россия, Санкт-Петербург, 14 линия, 39,
[2] ОАО «Воентелеком» Россия, Московская обл., г. Одинцово, ул. М.Говорова, д.14,
e-mails: vsaluhov@bk.ru, shevo-641@mail.ru.

Аннотация: В работе исследуются процессы анализа и снижения рисков при проектировании и строительстве телекоммуникационных систем. Приведен анализ возможностей применения основных известных способов и методик оценивания рисков проектирования и строительства телекоммуникационных систем, исследованы их достоинства и недостатки. Разработаны предложения, модели и методики для оценивания и снижения предпринимательских и техногенных рисков в условиях неопределенности, рисков нарушения безопасности программных средств.
Даны рекомендации по направлениям совершенствования экспертного оценивания и снижения рисков при проектировании и строительстве телекоммуникационных систем.

Ключевые слова: *телекоммуникационные системы; факторы рисков; анализ рисков; оценка рисков; безопасность.*

RISK MANAGEMENT AT VARIOUS STAGES THE LIFE CYCLE OF TELECOMMUNICATION SYSTEMS

Salukhov Vladimir[1], Shevchenko Oleg[2]
[1]St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint-Petersburg, 14th line, 39,
2 JSC «Voentelekom», Moscow region, Odintsovo, street Hovorova, 14,
e-mails: vsaluhov@bk.ru, shevo-641@mail.ru.

Abstract: This paper investigates the processes of analysis and reduce risks during design and construction of telecommunication systems. The analysis of possible applications of the main known methods and techniques for risk assessment of the design and construction of telecommunication systems, examines their advantages and disadvantages. Developed proposals, models and methodologies for the evaluation and reduction of entrepreneurial and technological risks under conditions of uncertainty, security risks software.
Recommendations for areas of improvement expert assessment and reduction of risks in the design and construction of telecommunication systems.

Keywords: *telecommunication systems; risk factors; risk analysis; risk assessment; security*

Введение. Проектирование и строительство телекоммуникационных систем вследствие влияния случайных факторов различного рода, наличия множества неопределенностей во всех аспектах деятельности подвержены многочисленным и разнообразным рискам. В наиболее общем и обобщенном виде риски характеризуют вероятность и возможные потери или убытки при реализации телекоммуникационной системы. При этом характер потерь и убытков может быть различным и выражаться как в денежной, так и в иной форме.

Задачи анализа, моделирования и управления рисками проектирования, строительства и функционирования телекоммуникационных систем являются актуальными для современного этапа создания подобных систем. Это обусловлено тем обстоятельством, что наличие рисков на этапах жизненного цикла сложных технологических систем приводит к неоправданным потерям или ущербу для заказчика и пользователей инфотелекоммуникационными услугами, окружающей среде, снижению эффективности целевого использования систем или даже к прекращению их функционирования. Поэтому одним из перспективных и востребованных направлений экспертного оценивания проектов телекоммуникационных систем может стать анализ уровня рисков проектов, оценка эффективности проектов и систем с учетом факторов рисков. В настоящее время этот аспект экспертной деятельности недостаточно исследован и не в полной мере отражен как в известной литературе, так и в отраслевой нормативной базе.

В работе анализируются основные положения действующей нормативной базы, научно-технической литературы по качественному и количественному анализу и оцениванию рисков сложных технологических систем, возможность их использования применительно к процессам проектирования и строительства сетей связи. Обосновываются подходы к выбору основных показателей для оценки рисков, рассматриваются модели и методическое обеспечение для оценивания и снижения различных видов предпринимательских и техногенных рисков в условиях неопределенности, рисков

нарушений информационной безопасности сетей связи, в том числе безопасности программных средств. Рассмотрены как методы качественного анализа, так и методы количественного оценивания рисков с учетом различного вида и состава имеющейся информации.

Сформулированы рекомендации по направлениям совершенствования экспертного оценивания и снижения рисков при проектировании и строительстве телекоммуникационных систем.

Реализация разработанных подходов к анализу рисков и расчету их количественных показателей может быть направлена как на повышение эффективности принятия проектных решений, так и на совершенствование экспертной деятельности по анализу проектов сетей связи. Результаты проведенных исследований могут быть использованы при поиске и обосновании путей снижения издержек при проектировании и строительстве телекоммуникационных систем в условиях существенной неопределенности на основе всестороннего анализа рисков и своевременного принятия мер, направленных на их минимизацию.

1. Обзор действующих требований и существующих подходов к анализу и управлению рисками телекоммуникационных систем

Проектирование и строительство телекоммуникационных систем сопряжены с множеством самых разнообразных неопределенностей, и, вследствие влияния случайных факторов различного рода, неизбежно подвержены рискам. В наиболее обобщенном смысле риски характеризуют возможные потери или убытки при реализации и функционировании телекоммуникационной системы, связанные с вероятными отклонениями по различным причинам тех или иных параметров, процессов, влияющих на ожидаемые результаты. Основополагающими нормативными документами федерального уровня [1], [2] в явном виде не предусмотрены задачи оценивания рисков проектирования и строительства телекоммуникационных систем. В то же время проведенный анализ путей обеспечения высокой эффективности создаваемых технологических систем, аналогичных по уровню сложности сетям связи, доказывает, что своевременно проведенные анализ и оценивание рисков их разработки и создания позволяют снизить расходы, предупредить принятие заведомо невыгодных проектных и иных решений. Для того, чтобы определить наиболее продуктивные направления использования подходов к оцениванию рисков проектирования и строительства телекоммуникационных систем, проанализируем требования основных действующих руководящих и нормативных документов по организации данного процесса. Первое, что необходимо сделать при данном анализе – установить наиболее пригодный для анализа, оценивания и управления рисками класс систем, рассматриваемых в нормативных документах по управлению рисками. Современные сети связи являются сложными технологическими системами, в состав которых входят разнообразные аппаратные и программные средства, используемые при оказании услуг связи и обеспечении функционирования сетей связи с участием эксплуатирующего персонала.

Перечень основных отечественных стандартов, определяющих требования и положения по организации и осуществлению риск-менеджмента на различных этапах жизненного цикла технологических систем, приведен в литературе [5], - [21].

Несомненно, что проекты по реализации телекоммуникационных систем относятся к классу инвестиционных проектов. Налицо наличие у этих объектов следующих признаков:

– необходимость привлечения крупных финансовых средств;

– многоэтапность и достаточно длительное время проектирования и строительства телекоммуникационных систем;

– длительное время функционирования объекта;

– необходимость обеспечения требуемой эффективности объекта в динамично изменяющихся условиях;

– значительная неопределенность на всех этапах жизненного цикла телекоммуникационных систем.

Поэтому для подавляющего большинства такого рода объектов, как телекоммуникационные системы, важнейшим свойством является экономическая эффективность, прежде всего – интегральная, которая характеризует экономическую эффективность проекта в целом [1]. В связи с этим целесообразно рассмотреть требования нормативных документов применительно к данному свойству. В настоящее время основными нормативными документами, на основе которых осуществляется оценивание интегральной экономической эффективности любого инвестиционного проекта, являются Федеральный закон «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений (№22-ФЗ от 02.01.2000 г.)» [22] и Методические указания по оценке эффективности инвестиционных проектов [23]. Для практического использования при оценивании рисков проекта телекоммуникационной системы особенно важны Методические рекомендации [23]. Этот документ содержит описание корректных (непротиворечивых и отражающих правила рационального экономического анализа действий хозяйствующих субъектов) методов расчета эффективности инвестиционных проектов, а также правила и расчетные процедуры по оцениванию влияния неопределенности и качественного и количественного оценивания рисков проекта. Требования представленных выше нормативных документов должны учитываться при

организации работ по управлению рисками при проектировании и строительстве телекоммуникационных систем, а также при экспертном анализе рисков проектов сетей связи с учетом особенностей анализируемых объектов и процессов.

Многочисленными исследованиями установлено, а соответствующими нормативными документами закреплено, что риски появляются тогда, когда на принятие решений влияют факторы неопределенности [23], [24] и др. Под неопределенностью проекта телекоммуникационной системы в целом можно понимать неполноту или неточность информации об условиях реализации проекта, в том числе о связанных с ними затратах и возможных получаемых результатах.

Неопределенность будущих результатов, например, обусловлена влиянием как множества экономических факторов (колебания рыночной конъюнктуры, цен, валютных курсов, уровня инфляции и т.п.), не зависящих от усилий участников проектирования телекоммуникационных систем, так и достаточного числа неэкономических факторов (климатические и природные условия, политические отношения и т.д.), которые не всегда поддаются точной оценке. Неопределенность прогнозируемых результатов приводит к возникновению риска того, что цели, поставленные в проекте телекоммуникационной системы, могут быть не достигнуты полностью или частично.

Учитывая сказанное, риски проектов телекоммуникационных систем следует рассматривать как результат воздействия на телекоммуникационную систему непредвиденных событий, которые с некоторой вероятностью (частотой появления) могут нанести ущерб проекту телекоммуникационной системы и препятствовать достижению целей ее проектирования, строительства и эксплуатации.

Таким образом, риск проекта телекоммуникационной системы характеризуется тремя основными составляющими, представленными на рисунке 1:

– событиями, оказывающими негативное воздействие на исследуемый проект телекоммуникационной системы;
– вероятностью появления таких событий;
– величиной ущерба, нанесённого проекту телекоммуникационной системы таким событием.

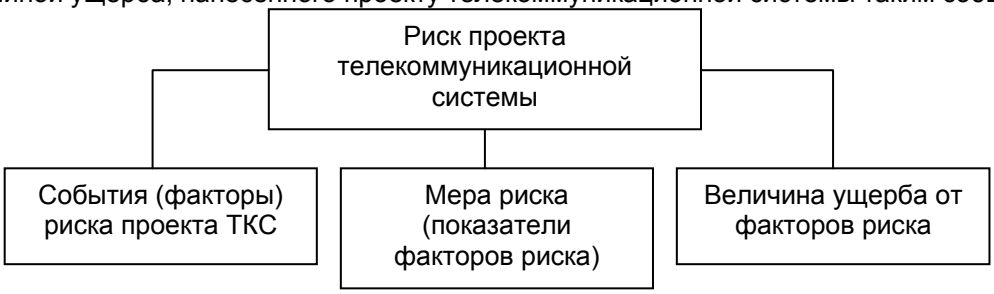


Рис. 1. Структура риска проекта

Первая составляющая риска формируется событиями, оказывающими негативное воздействие на исследуемый проект телекоммуникационной системы. К факторам риска относят, в общем случае, причины появления событий риска [25].

Вторая составляющая риска представляет собой количественное выражение уровня риска для проектирования и строительства телекоммуникационных систем по некоторой числовой шкале, определенное с помощью некоторого правила. Например, количественными показателями меры риска являются ожидаемая частота возникновения событий определенного типа или вероятность появления таких событий.

Величиной ущерба является количественная оценка возможных негативных последствий принимаемого решения при проектировании и строительстве телекоммуникационных систем, выраженная в тех или иных единицах в зависимости от назначения анализируемой системы и целей исследования. Во многих случаях ущерб от риска оценивается в материальной (денежной) форме. Однако могут быть случаи, когда потери носят такой характер, что оценить их в денежном выражении трудно, или невозможно, или нецелесообразно.

Можно сделать следующие выводы. Во-первых, риск, как правило, связан с принятием решения. Иначе говоря, именно необходимость принимать решения в условиях неопределённости порождает риск, а при отсутствии таковой необходимости нет и риска. Во-вторых, неопределённость объективна, а риск, чаще всего, субъективен. Например, объективное отсутствие достоверной информации о потенциальном объёме спроса на услуги связи приводит к возникновению совокупности рисков для участников проекта телекоммуникационной системы. Причём для каждого из участников проекта сети связи проявление риска индивидуально как в качественном, так и в количественном выражении.

В-третьих, поскольку неопределённость проекта телекоммуникационной системы выступает источником риска, её целесообразно минимизировать, например, посредством накопления и анализа дополнительной информации (пути снижения уровня неопределенности рассмотрены далее). Можно предположить, что в идеальном случае можно свести неопределённость к нулю, т.е. к полной определённости, за счёт получения качественной, достоверной, исчерпывающей информации об

условиях реализации проекта телекоммуникационной системы. Однако на практике этого сделать, как правило, не удаётся. Поэтому, оценивая при экспертизе риски проекта телекоммуникационной системы, необходимо некоторым образом учитывать и снижать уровень рисков применительно к условиям и способам описания существующей неопределённости проекта телекоммуникационной системы.

Рассмотрим основные виды рисков для проектирования и строительства телекоммуникационных систем [25], рисунок 2.

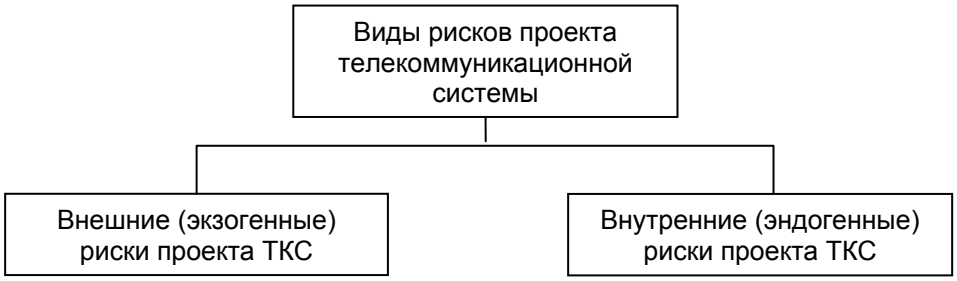


Рис. 2. Основные виды рисков проекта телекоммуникационной системы

Внешние (экзогенные) – риски, не связанные непосредственно с деятельностью участника проекта телекоммуникационной системы. К ним относятся, например, риски [22], [23]:

– вызванные изменениями экономической ситуации в стране и продуцируемые изменениями внешнеэкономической ситуации;
– связанные с нестабильной политической ситуацией или же с ее изменением;
– вызванные неадекватным законодательством;
– связанные с изменением природно-климатических условий (землетрясением, наводнением, другими стихийными бедствиями);
– генерируемые колебанием рыночной конъюнктуры,
– финансовые риски.

Для целей исследования, с учетом смысла используемых показателей интегральной эффективности проекта телекоммуникационной системы, важную роль играют риски последней группы. Финансовые риски – риски, обусловленные вероятностью потерь при проектировании и строительстве телекоммуникационной системы вследствие осуществления финансово-экономической деятельности в условиях неопределенности. К финансовымрискам относят риски колебаний покупательной способности денег (инфляционный, дефляционный, валютный).

Инфляционный риск проекта телекоммуникационной системы обусловлен, прежде всего, непредсказуемостью инфляции, поскольку ошибочный темп инфляции, заложенный в ставку дисконтирования, может существенно исказить значение показателя интегральной эффективности проекта. Говоря об инфляционном риске, следует отметить, что часто встречающиеся в литературе трактовки риска как того, что доходы будут обесцениваться быстрее, чем индексироваться, является некорректными. Такие риски по отношению к проекту телекоммуникационной системы неприемлемы, т.к. основная опасность инфляции заключается не столько в ее величине, сколько в ее непредсказуемости. При условии предсказуемости и определенности даже самую большую инфляцию можно легко учесть при проектировании телекоммуникационной системы либо в ставке дисконтирования, либо индексируя величину денежных потоков, сведя тем самым элемент неопределенности, а значит и риск, к нулю.

Валютный риск – риск потерь финансовых ресурсов вследствие непредсказуемых колебаний валютных курсов. Необходимо отметить, что даже самой твердой валюте присуща внутренняя инфляция, а динамика ее покупательной способности в отдельно взятой стране может быть весьма нестабильной.

Внутренние (эндогенные) – риски, которые связаны с деятельностью участника проекта телекоммуникационной системы. К ним относятся риски, вызванные [24], [25], [28]:

а) неполнотой или неточностью информации и исходных данных при разработке проекта телекоммуникационной системы, ошибками в проектной документации;
б) неадекватным подбором кадров, низким уровнем инвестиционного менеджмента;
в) ошибочной маркетинговой стратегией при анализе проекта телекоммуникационной системы;
г) перерасходом средств при проектировании и строительстве телекоммуникационных систем;
д) производственно-техническими нарушениями при реализации проекта;
е) некачественным управлением процессами проектирования и строительства телекоммуникационной системы;
ж) невыполнением контрактов и др.

Можно назвать и другие признаки, позволяющие осуществить классификацию рисков.

Риски проектирования и строительства телекоммуникационной системы для заказчика можно разделить на две основные группы (рисунок 3).

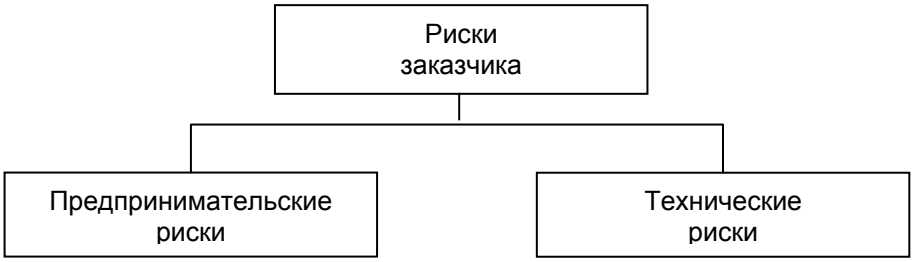


Рис. 3. Виды рисков заказчика

Предпринимательские риски связаны с несоответствием ожиданий заказчика в получении ожидаемой выгоды при реализации и использовании результатов проектной и инженерной деятельности при создании и использовании телекоммуникационной системы [23], [24]. Предпринимательский риск можно охарактеризовать как возможность того, что заказчик либо понесет потери в виде дополнительных расходов сверх предусмотренных проектом, либо получит доходы ниже тех, на которые он рассчитывал, либо получит прибыль при осуществлении выбранного какого-либо из альтернативных вариантов решения в условиях неопределенности, сопутствующей созданию и последующему использованию телекоммуникационной системы.

К техническим (техногенным) рискам будем относить возможные отрицательные исходы инженерной и производственной деятельности. Они могут возникнуть, например, при отклонениях фактических значений технических показателей проекта телекоммуникационной системы от их нормативных и проектных значений. Особенностью функционирования сети является то, что применительно к ней, как правило, не ставится задача превысить предусмотренные технико-экономические характеристики и целью функционирования является обеспечение достижения требуемых значений показателей этих характеристик при безопасной реализациипроекта. Поэтому технические риски, в отличие от рисков предпринимательских, имеют только негативные последствия.

Источниками этой группы рисков являются различные опасности или угрозы жизнедеятельности или благосостоянию человека, объектам хозяйства и окружающей среде с различными социальными, техническими, экономическими и экологическими последствиями. К техническим рискам относят также ситуации любых возможных отрицательных исходов функционирования оборудования телекоммуникационной системы. Применительно к техническим рискам, в первую очередь, речь идет о безопасности объектов.

2. Общая характеристика задач управления рисками при проектировании и строительстве сетей связи

Процессы проектирования, строительства и функционирования сетей связи связаны с множеством самых разнообразных неопределенностей, и поэтому подвержены самым разнообразным рискам. Это обусловлено, прежде всего, сложностью и многогранностью как самих сетей связи, так и процессов их создания, применения и эксплуатации. Для современных сетей связи как объектов управления рисками, а также процессов их проектирования и строительства, характерны следующие основные особенности:

– большая продолжительность жизненного цикла сетей связи и отдельных этапов жизненного цикла;

– высокая структурная, функциональная, технологическая и техническая сложность сетей связи;

– наличие в составе сетей различных как технических, так и программных средств, широкая номенклатура применяемых изделий, оборудования, программных средств, материалов;

– применение в составе средств сетей связи оборудования и изделий как отечественного, так и импортного производства;

– сложная топологическая структура, большая территориальная рассредоточенность элементов сетей связи, больная протяженность линий связи;

– участие человека на всех этапах процессов проектирования, строительства и эксплуатации сетей связи, большое число участников процессов создания и применения сетей связи;

– другие особенности.

Задачи минимизации или снижения рисков при проектировании и строительстве телекоммуникационных систем являются составными частями процесса управления (менеджмента) рисками. В рамках решения задач минимизации рисков при проектировании и строительстве сетей связи основными являются процедуры количественной оценки рисков для различных вариантов проекта сети связи (или сценариев его реализации), и выбора варианта, обеспечивающего

минимальную величину рисков при заданных ограничениях. Применительно к задачам проектирования и строительства сетей связи общую процедуру решения задач оценки и снижения рисков следует рассматривать в соответствии с положениями и требованиями документов [7], [9], [21].

В наиболее обобщенном виде процесс менеджмента рисков включает две основные стадии: уяснение проблемы и ее решения [21]. На первой стадии основное внимание концентрируют на определении масштаба риска, подлежащего менеджменту, и идентификации риска. На второй стадии проводят окончательную оценку и осуществляют снижение риска. При этом на практике, как правило, менеджмент рисков является итеративным процессом, включающим в себя чередование этих стадий, поэтому жесткого различия между этими стадиями проводить не рекомендуется.

Более детально составляющие процесса управления рисками приведены на рисунке 4, и, соответственно, управление рисками включает в себя три основных составных части: анализ рисков, оценивание рисков и их обработку [7], [9], [21]. При этом общий процесс анализа риска и оценивания риска в соответствии с принятой терминологией представляет собой оценку риска.

Анализ риска включает в себя определение области применения, идентификацию опасности и оценку величины риска. Определение области применения анализа риска должно включать в себя: описание оснований и/или проблем, повлекших проведение анализа риска, описание исследуемой системы связи, ее контактов со смежными системами и окружающей средой, описание источников информации о факторах рисков и опасности, описание имеющихся предположений и ограничений, требований к результатам и выходным данным и пр. На этом этапе также должны быть заданы критерии риска – правила, по которым определяется значимость риска. Выбор критериев является сложной и ответственной задачей. Применительно к задачам проектирования и строительства сетей связи критерии должны отражать как технические требования к проектируемой сети, так и экономические интересы участников процесса. При формировании критериев необходимо учесть, что полностью устранить все риски принципиально невозможно, поэтому следует определить, какой уровень риска может быть принят за приемлемый или допустимый.

Цель идентификации опасностей состоит в определении и описании всех видов опасностей, являющихся причиной риска при проектировании и строительстве сети и способных повлиять на выполнение проекта в целом или на достижение целей отдельных стадий проекта. Этап идентификации опасностей и рисков является чрезвычайно важным, поскольку именно на этом этапе определяется круг рассматриваемых в дальнейшем видов рисков. Поэтому на данном этапе необходимо наиболее полно и адекватно определить все существенные виды опасностей. При этом следует рассматривать воздействия риска на все цели проекта, включая стоимость, время и качество, а также цели, связанные с необходимостью обеспечения требований законодательства, надежности, безопасности и пр.

Процедура оценки величины риска представляет собой процесс определения значений вероятности и последствий риска, т.е. количественную оценку риска. Количественная оценка риска является одним из наиболее сложных и трудоемких процессов и требует применения соответствующих (как правило, количественных) методов. Для проектов сложных технических систем, к каким относятся и сети связи, зачастую требуется разработка и применение специальных моделей, позволяющих адекватно описать механизмы воздействия опасностей и возникновения неблагоприятных последствий. На их основе произвести количественную оценку вероятностных характеристик, а также показателей, характеризующих степень последствий, размер вызываемого ущерба. При этом должны быть адекватно учтены все виды потенциальных опасностей, природа и механизмы их воздействия, причинно-следственные связи, возможные взаимозависимости между различными вирами опасностей и последствий и пр. Всё это требует использования большого объема исходной информации об исследуемой системе связи и процессах ее создания и функционирования. Следует при этом понимать, что полученные при количественной оценке расчетные значения риска представляют собой оценки, точность которых связана с точностью используемых данных и методов.

Следующим этапом управления рисками является оценивание рисков - процесс сравнения количественно оцененного риска по заданным критериям риска для определения значимости риска. При этом правила, по которым оценивают значимость риска (критерии), должны быть сформированы на начальном этапе анализа и могут включать в себя сопутствующие стоимость и выгоды, законодательные и обязательные требования, социально-экономические и экологические аспекты, озабоченность причастных сторон, приоритеты и др. По результатам оценивания рисков с учетом принятых критериев должно быть установлено, является ли рассчитанный риск данного типа приемлемым (и, соответственно, дополнительных мероприятий по его обработке не требуется), или величина риска превосходит допустимые значения. В последнем случае должны быть проведены дальнейшие процедуры по обработке риска. При наличии различных видов идентифицированных ранее рисков, по результатам оценивания также определяются приоритеты для их обработки.

Обработка рисков включает в себя анализ и принятие необходимых ответных мер, способствующих минимизации рисков. Обработка риска производится с целью идентификации и

осуществления рентабельных действий, которые позволят сделать риск приемлемым (допустимым). Обработка риска может включать в себя действия, направленные на:

- полное устранение или предупреждение риска;
- уменьшение вероятности появления опасного события;
- уменьшение последствий опасного события;
- перемещение или распределение риска;
- сохранение риска и разработку планов устранения последствий.

Следует учитывать, что при обработке риска могут быть сгенерированы новые виды риска, которые также следует идентифицировать и аналогично рассматривать. Вариант обработки риска (или комбинацию вариантов) следует выбирать на основе анализа рентабельности затрат на обработку или устранение риска вместе с потенциальными выгодами результатов от выполнения этих вариантов обработки. Риск, который остается после действий по его снижению, может быть передан или распределен между теми, кто его оплачивает, например, субподрядчиками или страховыми компаниями. В некоторых случаях возможна полная передача риска. При решении задач минимизации рисков при проектировании и строительстве сетей связи по результатам выполнения данного этапа из множества всех допустимых вариантов должен быть выбран такой вариант, при котором обеспечивается минимальная величина рисков при выполнении заданных требований и ограничений.

Поскольку полностью устранить все виды рисков невозможно, должны предусматриваться действия по ликвидации последствий в предположении, что опасное событие произошло. Эти планируемые действия следует выполнять в случае реализации опасного события. Такие действия могут составлять, например, стратегию восстановления объектов сетей связи, включающую порядок устранения отказов, порядок действий и состав обслуживающего персонала, номенклатуру запасных частей, инструмента и принадлежностей и т.д. Стратегия восстановления может включать в себя также, к примеру, порядок и содержание действий при нарушениях информационной безопасности, несанкционированном доступе к объектам сети связи и информации и пр.

Описанная процедура имеет общий методологический характер, конкретное же наполнение ее этапов конкретизируется и детализируется в зависимости от особенностей рассматриваемых объектов и процессов, имеющейся информации, целей исследования и прочих факторов.

3. Подходы и методы оценки и снижения предпринимательского риска проектирования и строительства сетей связи в условиях ограниченности информации

При проектировании и строительстве телекоммуникационных систем имеют место предпринимательские риски, которые могут быть связаны с несоответствием ожиданий в получении предполагаемой выгоды при реализации и использовании результатов проектной деятельности, возможностью понести потери в виде дополнительных расходов сверх предусмотренных проектом, либо получить доходы ниже запланированных и прочими причинами, обусловленными наличием множества неопределенностей, сопутствующих созданию и последующему использованию телекоммуникационной системы.

При оценке предпринимательских рисков при проектировании и строительстве телекоммуникационных систем широко используются, как это уже отмечалось в предыдущих разделах, показатели и критерии экономической эффективности. В том числе, распространенное применение имеют критерии интегральной эффективности реализуемого проекта телекоммуникационной системы.

При оценке предпринимательских рисков проектирования и строительства сетей связи должна использоваться вся имеющаяся информация об условиях реализации проекта, в том числе и не выражающаяся в количественной форме. Поэтому в таких задачах широко применяются как качественные, так и количественные методы анализа и оценивания рисков.

При качественном оценивании рисков проектирования и строительства телекоммуникационных систем наибольшее распространение получили следующие методы [23], [24], [25]:

- метод анализа уместности затрат;
- метод аналогий;
- метод экспертных оценок.

Помимо методов качественного анализа, для получения количественных оценок рисков широко используются методы количественного анализа. Основной целью количественного подхода при оценивании рисков проекта телекоммуникационной системы является численное оценивание влияния факторов риска на поведение критериев эффективности проекта и соответствующее обоснование необходимых мер по снижению уровня рисков проекта. Проведенный анализ показал, что наиболее пригодны для количественного оценивания рисков проектирования и строительства телекоммуникационных систем следующие количественные методы [22], [23], [25]:

- статистический метод;
- метод анализа чувствительности проекта (метод вариации параметров);
- метод проверки устойчивости проекта (расчет критических точек);

– метод сценариев (метод формализованного описания неопределенностей проекта);
– имитационное моделирование (метод статистических испытаний, метод Монте-Карло);
– метод корректировки ставки дисконтирования.

Природа неопределённости условий реализации проекта формируется под воздействием различных факторов [24], [33], к которым можно отнести следующие:

– неопределённость по фактору времени, которая обусловлена тем, что невозможно с достоверностью до единицы предсказать значение того или иного фактора риска в будущем;
– неопределённость рыночной конъюнктуры, обусловленная неизвестностью точных значений параметров рыночной системы;
– непредсказуемость поведения участников проекта телекоммуникационной системы и т.д.

Сочетание этих факторов на практике создаёт обширный спектр различных видов неопределённости.

Неопределенность ситуации и условий реализации проекта может быть задана по-разному [23]:

– в виде вероятностных распределений (распределение случайной величины показателя эффективности точно известно, но неизвестно, какое именно значение примет этот показатель, что должно оцениваться экспертным способом);
– в виде субъективных вероятностей (распределение случайной величины неизвестно, но известны вероятности отдельных событий, определённые экспертным путём);
– в виде интервальной неопределённости (распределение случайной величины неизвестно, но известно, что она может принимать любое значение в определённом интервале).

Рассмотрим последовательность оценивания ожидаемого эффекта проекта телекоммуникационной системы с учетом количественных характеристик неопределенности. При этом будем опираться на метод сценариев. Предполагается, что необходимо оценить интегральный показатель эффективности проектирования и строительства телекоммуникационной системы - ожидаемый интегральный эффект (ожидаемый доход). Оценка ожидаемой эффективности проекта с учетом неопределенности производится при наличии информации о различных сценариях реализации проекта, вероятностях их осуществления и о значениях основных технико-экономических показателей проекта при каждом из сценариев.

Расчеты необходимо осуществлять в следующем порядке:

1) описывается все множество возможных сценариев реализации проекта телекоммуникационной системы (либо в форме перечисления, либо в виде системы ограничений на значения основных технических, экономических и других параметров проекта);
2) по каждому сценарию исследуется, как будет действовать в соответствующих условиях организационно-экономический механизм реализации проекта, как при этом должно осуществляться изменение денежных потоков участников проекта телекоммуникационной системы;
3) для каждого сценария по каждому шагу расчетного периода определяются (рассчитываются либо задаются аналитическими выражениями) притоки и оттоки денежных средств (включая денежные потоки, связанные с взаимными санкциями участников, страхованием, резервированием и иными элементами организационно-экономического механизма реализации проекта в условиях рисков) и обобщающие показатели эффективности. По сценариям, предусматривающим «нештатные» ситуации (аварии, стихийные бедствия, резкие изменения рыночной конъюнктуры и т.п.), учитываются соответствующие риски и возникающие при этом дополнительные затраты. При определении чистого дисконтного дохода (ЧДД) по каждому сценарию норма дисконта принимается безрисковой;
4) экспертно проверяется финансовая реализуемость проекта. Нарушение условий реализуемости рассматривается как необходимое условие прекращения проекта (при этом учитываются потери и доходы участников, связанные с прекращением создания телекоммуникационной системы по причине его финансовой несостоятельности);
5) исходная информация о факторах неопределенности представляется в форме вероятностей отдельных сценариев или интервалов изменения этих вероятностей. Тем самым определяется некоторый класс допустимых (согласованных с имеющейся информацией) вероятностных распределений показателей эффективности проекта. В частных случаях этот класс может состоять из единственного вероятностного распределения или из всех распределений на множестве возможных сочетаний показателей эффективности;
6) оценивается риск нереализуемости проекта телекоммуникационной системы; количественно этот риск характеризуется суммарной вероятностью сценариев, при которых нарушаются условия финансовой реализуемости проекта;
7) оценивается риск неэффективности проекта, который количественно характеризуется суммарной вероятностью сценариев, при которых интегральный эффект (ЧДД) становится отрицательным;
8) оценивается средний ущерб от реализации проекта в случае его неэффективности;
9) на основе показателей отдельных сценариев определяются обобщающие показатели эффективности проекта с учетом факторов неопределенности - показатели ожидаемой

эффективности. Основными такими показателями, используемыми для сравнения различных проектов (вариантов проекта) и выбора лучшего из них, являются показатели ожидаемого интегрального эффекта (ЧДД) (общественной эффективности и коммерческой эффективности для отдельного участника). Эти же показатели используются для обоснования рациональных размеров и форм резервирования и страхования при минимизации идентифицированных рисков проекта телекоммуникационной системы.

Порядок определения показателей ожидаемого эффекта проектирования телекоммуникационной системы в условиях рисков зависит от способа задания и имеющейся информации о неопределенностях условий реализации проекта. В следующем подразделе рассмотрены наиболее важные случаи – случай учета вероятностной неопределенности и случай учета интервальной неопределенности по сценариям проекта.

При вероятностной неопределенности по каждому сценарию считается известной (заданной) вероятность его реализации [21], [22]. Вероятностное описание условий реализации проекта оправдано и применимо, когда эффективность проекта обусловлена неопределенностью объективных условий размещения проектируемой телекоммуникационной системы или процессов эксплуатации и износа основных средств (снижение прочности конструкций зданий и сооружений, отказы оборудования и т.п.).

В случае, когда имеется конечное количество сценариев и вероятности их заданы, ожидаемый интегральный эффект проекта рассчитывается по формуле суммы произведений интегральных эффектов (ЧДД) по каждому сценарию на вероятности реализации этих сценариев.

При этом риск неэффективности проекта телекоммуникационной системы определяется как сумма вероятностей сценариев, для которых интегральные эффекты (ЧДД) отрицательны. Средний ущерб от реализации проекта телекоммуникационной системы в случае его неэффективности определяется как сумма произведений абсолютных значений ЧДД для сценариев, для которых интегральные эффекты (ЧДД) отрицательны, навероятности этих сценариев.

Интегральные эффекты сценариев и их ожидаемый эффект зависят от значения используемой нормы дисконта. Значение указанного параметра должно учитываться при формировании так называемой премии за риск неполучения доходов, предусмотренных основным сценарием проекта телекоммуникационной системы. Значение премии за риск определяется из условия равенства между ожидаемым эффектом проекта, рассчитанным при безрисковой норме дисконта, и эффектом основного сценария, рассчитанным при норме дисконта, включающей поправку на риск [23], [31].

В этом случае средние потери от неполучения предусмотренных основным сценарием доходов при неблагоприятных сценариях покрываются средним выигрышем от получения более высоких доходов при благоприятных сценариях. Таким образом, размер премии за риск зависит от того, какой сценарий принят в качестве базисного.

В практике проектирования и строительства телекоммуникационной системы встречаются ситуации, когда какая-либо информация о вероятностях сценариев отсутствует (известно только, что они положительны и в сумме составляют единицу). Рассмотрим, как в таких случаях осуществить расчет ожидаемого интегрального эффекта проекта телекоммуникационной системы [23], [28].

1 этап. Экспертным путем определяется наибольшее и наименьшее значения показателей интегрального эффекта (ЧДД) по рассмотренным сценариям развития проекта телекоммуникационной системы.

2 этап. Вводится специальный норматив для учета неопределенности эффекта, отражающий систему предпочтений заказчика (участников) проекта телекоммуникационной системы в условиях неопределенности.

3 этап. Ожидаемый интегральный эффект проекта телекоммуникационной системы рассчитывается из соотношения, представляющего собой сумму, слагаемыми которой являются а) произведение норматива на наибольшее значение показателя интегрального эффекта (ЧДД); б) произведение разности единицы и норматива на наименьшее значение показателя интегрального эффекта (ЧДД).

При определении ожидаемого интегрального экономического эффекта от реализации проекта телекоммуникационной системы рекомендуется норматив принимать на уровне 0,3.

Таким образом, на основе применения рассмотренных методик расчетов значений показателя интегрального эффекта (ЧДД) в условиях неопределенности различного вида становится возможным существенно снизить предпринимательские риски проектирования и строительства телекоммуникационной системы путем введения соответствующих «премий за риск».

4. Анализ рисков нарушения безопасности программных средств сети связи

Применительно к функционированию программных средств, как неотъемлемой составляющей сетей связи, особую значимость имеет фактор наличия опасности преднамеренных и непреднамеренных воздействий нарушителей на передаваемую информацию, информацию управления, данные пользователей, а также сами средства сетей связи, обеспечивающие эти процессы. Поэтому в рамках общей задачи оценивания рисков проектирования и строительства сетей

связи необходимым является рассмотрение рисков, связанных с нарушениями информационной безопасности сетей связи, в том числе безопасности программных средств.

В предметной области обеспечения безопасности программных средств используются термины и определения, содержащиеся в стандартах ГОСТ 27.002-89, ГОСТ 28806-90, ГОСТ Р ИСО/МЭК 9126-93, ГОСТ 28195-89 и ряде других документов.

Под безопасностью сети связи понимается свойство сети связи противостоять угрозам негативных неумышленных и умышленных несанкционированных воздействий на сеть связи и ее отдельные объекты (в том числе – программные средства) в заданных режимах и условиях ее функционирования. Факты таких несанкционированных воздействий на сеть связи и ее отдельные объекты (в том числе – программные средства) являются нарушениями безопасности. Нарушитель (нарушители) – субъект (субъекты), совершающие несанкционированный доступ к программному средству сети связи и (или) информационному ресурсу, используемому программным средством.

Программное средство (software) – это объект, состоящий из программ, правил, процедур, а также, если предусмотрено, соответствующих им документации и данных, относящихся к функционированию системы обработки информации. Программное средство (ПС) представляет собой конкретную информацию, объективно существующую как совокупность всех значимых с точки зрения ее представления свойств каждого из материальных объектов, содержащих в фиксированном виде эту информацию.

Программно-аппаратное средство (firmware) – это сочетание технических устройств и машинных команд или используемых вычислительной машиной данных, постоянно хранящихся на техническом устройстве в виде программного средства. Компьютерная программа и данные, входящие в программно-аппаратные средства, классифицируются как программное обеспечение; схемы, содержащие компьютерную программу и данные, классифицируются как технические средства.

Обеспечение безопасности программных средств сети связи является составной частью общей проблемы обеспечения информационной безопасности телекоммуникационных систем.

Соответственно, под риском нарушения информационной безопасности сети связи следует понимать сочетание вероятности события, заключающегося в преднамеренных и непреднамеренных воздействиях нарушителей на передаваемую информацию, информацию управления, данные пользователей, а также сами средства сетей связи, и последствий таких воздействий. Риском нарушения безопасности программных средств будет являться сочетание вероятности преднамеренных и непреднамеренных воздействий на программные средства, и последствий таких воздействий, относящихся к функционированию систем передачи, обработки и хранения информации.

Деятельность по обеспечению безопасности программных средств является составной частью работы по управлению рисками проектирования, создания и функционирования сетей связи, направленной на снижение уровня риска до допустимого.

В организации мероприятия по обеспечению безопасности следует регламентировать в виде программы обеспечения безопасности (ПОБ), которая является документом, устанавливающим комплекс взаимосвязанных организационно-технических требований и мероприятий, подлежащих проведению на определенных стадиях жизненного цикла объекта и направленных на обеспечение заданных требований к безопасности и/или на повышение безопасности программных средств. ПОБ должна устанавливать цели мероприятий на каждом этапе жизненного цикла программных средств, применяемые нормативные документы и методики, сроки выполнения мероприятий и исполнителей, порядок оформления и контроля результатов оценивания уровня безопасности программных средств сети связи.

Под оценкой безопасности программных средств понимается процесс получения количественных или качественных показателей при учете преднамеренных и непреднамеренных воздействий и дефектов в программном средстве сети связи.

Основными объектами обеспечения безопасности в информационных и телекоммуникационных системах являются:

– информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

– средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа;

– технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации.

Основными угрозами безопасности в сетях связи являются:

– деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием сетей связи;

– вынужденное в силу объективного отставания отечественной промышленности использование импортных программно-аппаратных средств при создании и применении сетей связи;

– нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала сетей связи, отказы технических средств и сбои программных средств;

– использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты процессов переработки информации и контроля их эффективности;

– привлечение к работам по созданию, развитию и защите сетей связи фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Одной из важнейших функций всех типов сетей связи, является функция управления. В настоящее время эта функция реализуется со все большим применением программного обеспечения сети связи. Эта роль программных средств будет неуклонно возрастать.

Очевидно, что информация, циркулирующая в структуре сети связи и обеспечивающая выполнение функций сети, требует обеспечения ее защиты и безопасности сети связи.

Программные средства сетей связи, используемые различными категориями операторов связи, хотя и существенно различается по функциям и, соответственно по своей структуре, но требования, предъявляемые к безопасности их функционирования, достаточно высоки.

Программные средства сетей связи представляют собой разнородные программные комплексы, имеющие развитую и сложную архитектуру. При этом они отличаются программными платформами, на базе которых они создаются. Все типы программных средств сетей связи полностью соответствуют представлению о них, как продуктах промышленного производства.

Угрозы безопасности информации и программных средств сетей связи возникают как в процессе их эксплуатации, так и при проектировании и создании этих систем, что особенно характерно для процесса разработки ПО, баз данных и других информационных компонентов сети связи.

Перечень угроз, оценки вероятностей их реализации, а также модель угроз являются основой для определения требований к системе защиты. На практике задача формального описания полного множества угроз чрезвычайно сложна вследствие очень большого числа факторов, влияющих на процессы обмена информацией в современных сетях связи. Поэтому для анализируемой сети связи определяют, как правило, не полный перечень угроз, а перечень классов угроз в соответствии с принятой классификацией. При этом классификация возможных угроз безопасности программных средств сети связи проводится по ряду базовых признаков, к которым можно отнести следующие:

– природа возникновения угроз;
– степень преднамеренности проявления;
– непосредственный источник угроз;
– местонахождения источника угроз;
– степень зависимости источников угроз от активности функционирования программных средств сети связи;
– степени воздействия на программные средства сети связи и т.п.

Нарушение требований по безопасности программных средств сетей может быть обусловлено следующим угрозами функционирования сетей связи на территории нашей страны [31], [32]:

– противоправные сбор и использование информации;
– нарушения технологии обработки информации;
– внедрение в аппаратные и программные средства компонентов, реализующих функции, не предусмотренные документацией на эти средства;
– разработка и распространение программ, нарушающих нормальное функционирование сетей связи, в том числе и их систем защиты информации;
– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникаций и связи;
– воздействие на парольно-ключевые системы защиты сетей связи и других автоматизированных систем обработки и передачи информации;
– компрометация ключей и средств криптографической защиты информации;
– утечка информации по техническим каналам;
– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций;
– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации.

Основные факторы угроз безопасности программных средств сети связи выступают как возможные опасности ухудшения качества обслуживания пользователей в сети связи вследствие воздействий нарушителя на информационную сферу сети связи. Угрозы безопасности реализуются через уязвимости сети связи. Любое успешное воздействие нарушителя, направленное на реализацию угрозы безопасности сети и ее программных средств, как установлено из практики функционирования сетей связи, как правило, опирается на полученные нарушителем знания об особенностях построения и уязвимостях сети связи.

5. Рекомендации по совершенствованию экспертного оценивания и снижения рисков при проектировании и строительстве телекоммуникационных систем

Экспертная деятельность является одним из реально применимых способов снижения уровня неопределенности, приводящей к появлению рисков принятия неверных или неэффективных решений при проектировании и строительстве сетей связи. Поэтому совершенствование экспертной деятельности в направлении анализа и оценивания уровня эффективности рисковых проектов является важной задачей, направленной на поиск и обоснование путей снижения издержек при проектировании и строительстве телекоммуникационной системы в условиях существенной неопределенности.

После того, как проанализированы и выявлены риски в проекте телекоммуникационной системы, экспертам необходимо проанализировать и оценить правильность и достаточность принятых решений по минимизации рисков и дать рекомендации по снижению рисков по этапам проектирования и строительства телекоммуникационной системы.

В анализируемом проекте телекоммуникационной системы должны содержаться решения и рекомендации по мерам, направленным на снижение рисков проектирования и строительства, разработанным проектной или иной организацией, участвующей в подготовке и реализации проекта. На этапе подготовки экспертного заключения об уровне эффективности разработанного проекта необходимо оценить правильность и практическую осуществимость предлагаемых в проекте мер снижения инвестиционного риска реализуемого проекта. На основании полученных результатов количественного оценивания факторов рисков проекта телекоммуникационной системы должно быть получено экспертное заключение о том, насколько целесообразна реализация данного проекта телекоммуникационной системы с учетом планируемых мероприятий по управлению рисками. Рассмотрим, как возможно решать такую задачу на этапе экспертизы.

Основной принцип действия механизма по снижению рисков проектирования и строительства телекоммуникационных систем состоит в комплексности (по характеру своего воздействия) и экономической целесообразности предлагаемых для реализации мер. Экспертным путем должны быть проанализированы классические мероприятия по управлению рисками, в том числе по обработке рисков, которые могут подразделяться на следующие группы [22,26]:

– принятие риска – риск принимается, если все доступные способы его снижения не являются экономически целесообразными по сравнению с ущербом, который может нанести реализация риска. (Напомним, что принятие риска – это решение принять риск. Принятие риска зависит от критериев риска.) При проведении экспертизы проекта экспертной группе следует убедиться в том, что проектная организация и заказчик осведомлены о наличии данного риска и его характеристиках и осознанно не принимает каких-либо мер по воздействию на риск проекта телекоммуникационной системы;

– избежание риска – реализуется путем выработки рекомендаций либо о мероприятиях, позволяющих устранить рассматриваемый вид риска, либо о прекращении деятельности по проекту в том виде, в каком он представлен на экспертизу; во втором случае по своей сути данное заключение экспертизы будет означать необходимость отказа от проекта телекоммуникационной системы;

– передача риска – решение о передаче риска зависит от характера риска, важности связанной с риском операции и ее значимости для параметров проекта. Стандартные механизмы передачи рисков включают: страхование строительных и монтажных рисков, перераспределение рисков между участниками проектирования и строительства сети связи, передачу рисков партнерам в рамках проектных контрактов, аутсорсинг, хеджирование;

– контроль/снижение риска – достигается с помощью внедрения дополнительных организационных и контрольных процедур по проекту, например, разработки мероприятий по обеспечению непрерывности функционирования проектируемой сети связи, безопасности телекоммуникационной системы в процессе работы и в опасных ситуациях при функционировании и т.д.;

– возможность покрытия непредвиденных расходов – в этом случае экспертно устанавливается целесообразность создания резервных фондов (по каждому этапу проектирования и строительства телекоммуникационных систем);

– снижение финансовых рисков – осуществляется экспертное оценивание возможности достижения положительного сальдо имеющихся средств на каждом шаге реализации проекта телекоммуникационной системы;

– оценка наличия системы гарантий – экспертно следует проанализировать возможность получения для реализации проекта телекоммуникационной системы гарантий государства, банка, инвестиционной компании и т.п.;

– снижение уровня неопределенности проекта – при проведении экспертизы необходимо убедиться в том, что предусматривается возможность и средства получения дополнительной информации о воздействующих факторах;

– сохранение риска и разработка планов устранения последствий – необходимо убедиться в том, что для тех видов рисков, которые сохраняются, предусматриваются действия, планы мероприятий по ликвидации последствий в предположении, что опасное событие всё же произошло.

Процесс экспертного анализа и управления рисками проектов телекоммуникационных систем условно можно разделить на два основных этапа.

К основным процедурам первого этапа, реализуемого на стадии принятия решения об инвестировании в новый проект телекоммуникационной системы, относятся выявление, первичная оценка рисков проекта и разработка возможных мер по управлению рисками и их снижению.

Второй этап, реализуемый на стадии строительства телекоммуникационной системы, включает в себя мониторинг развития рисковых ситуаций и контроль исполнения разработанных мероприятий по управлению рисками. Соответственно, и класс рисков здесь принципиально иной: на стадии принятия решения о возможности реализации проекта новой сети связи они носят стратегический характер, а на стадии реализации проекта (этапе строительства телекоммуникационной системы) – чисто операционный.

Риски внешней и риски внутренней среды проекта телекоммуникационной системы должны учитываться путем использования единых сценарных условий, которые включают в себя перечень наиболее значимых показателей, а также условий и допущений, необходимых для проведения расчета параметров экономической эффективности всех вариантов рассматриваемых заказчиком проектов новых телекоммуникационных систем. При этом могут быть предложены следующие методические рекомендации.

При анализе проекта сценарные условия могут формироваться на долгосрочный период (например, на 25 лет) по нескольким стандартным вариантам (например, трем: консервативному, умеренному, оптимистическому). Уточнения и дополнения должны вноситься в плановом порядке, либо с установленной периодичностью или внепланово в случае существенной корректировки используемых показателей в связи с нововведениями в действующем законодательстве или другими изменениями условий деятельности. Сценарные условия следует формировать на основании двух источников информации – внешнего, включая прогнозы государственных органов власти, и внутреннего, включая фактические данные, которые могут предоставляться как проектирующей организацией, так и заказчиком проекта, оператором проектируемой сети связи или эксплуатирующей организацией.

В сценарных условиях необходимо отражать такие параметры, как индекс инфляции и индексы-дефляторы инвестиций, промышленной продукции и зарплаты, курсы иностранных валют относительно рубля, процентные ставки привлечения долгосрочных кредитов, цены на электроэнергию и мощность, и т.д. Использование единых сценарных условий позволяет унифицировать и значительно упростить экспертную оценку эффективности проектов. При этом обеспечивается учет рисков внешней среды проекта.

Как уже установлено ранее, ко второй группе относятся риски изменения различных специфичных факторов, свойственных проектам телекоммуникационных систем и оказывающих большое влияние на значения их финансовые показателей. Это технологические и технические, затратные, экологические риски, риски задержек и ошибок при принятии управленческих решений, экономические и другие виды рисков, присущих проекту телекоммуникационной системы на всех стадиях его жизненного цикла.

Для повышения безопасности программных средств сети связи при экспертизе проектной документации можно рекомендовать применять разработку программы обеспечения безопасности анализируемых средств сети связи, аналогичную программе обеспечения надежности (ПОН) этих средств. В этом случае на основании договора о разработке проекта сети связи указанный документ может разрабатываться после утверждения задания на проектирование сети связи, включающего раздел по нормированию требований по безопасности программных средств сети.

Проект документа может включать в себя перечень необходимых организационных и технических мероприятий для управления безопасностью программных средств сети связи при проектировании и разработке сети связи на всех этапах ее жизненного цикла. При этом управление включало бы в себя функции планирования, координации и контроля выполнения работ по обеспечению безопасности программных средств сети связи.

Для выполнения перечисленных задач возможно создание системы управления безопасностью программных средств сети связи. Требования к системе управления безопасностью программных средств сети связи по согласованию между заказчиком и поставщиком можно было бы включать в условия договора на проектирование сети связи.

В рассматриваемом случае с помощью проекта программы обеспечения безопасности сети связи предлагается предусматривать следующие мероприятия:

– сбор и анализ всей доступной информации о безопасности и угрозах безопасности программных средств, используемых при создании различных проектов сетей связи, как отечественных, так и зарубежных производителей, создание и ведение базы данных по угрозам программным средствам сети связи;

– обоснование значений показателей качества программных средств сети связи с учетом требований по их безопасности;

– выбор и обоснование предполагаемых типов программных средств, обеспечивающих решение целевых задач, поставленных перед сетью связи, а также возможных поставщиков выбранных типов программных средств;

– распределение требований по безопасности между программными и аппаратными средствами сети связи и включение соответствующих требований в частные технические задания;

– выбор и обоснование возможных способов обеспечения безопасности сети связи в целом;

– обоснование методов расчета показателей безопасности программных средств сети связи для оценки при экспертизе проекта соответствия разрабатываемого варианта требованиям по безопасности;

– планирование и разработка методов экспериментальной оценки показателей безопасности программных средств сети связи с использованием специальных испытательных имитационных стендов и по результатам опытной эксплуатации сети связи;

– разработка, изготовление или приобретение испытательного стенда, имитирующего работу сети связи, для проведения испытаний программных средств сети связи на безопасность в период до создания сети связи;

– проведение экспериментальных исследований на испытательном стенде и получение предварительных оценок показателей безопасности программных средств, выполнение анализа выявленных угроз безопасности программных средств, проведение необходимых доработок программных средств;

– обоснование перечня мер по обеспечению требуемой безопасности программных средств сети связи, включаемых в эксплуатационную документацию на программные средства;

– расчет и обоснование необходимых ресурсов, с использованием которых планируется осуществлять мероприятия по обслуживанию и сопровождению программных средств сети связи;

– выбор и обоснование оптимальных способов обслуживания и сопровождения программных средств сети связи;

– применение установленных мер системы государственного регулирования в области обеспечения безопасности программных средств сети связи (обеспечения лицензирования, сертификации и аттестации всех участников жизненного цикла сети связи);

– обоснование экономической целесообразности обеспечения безопасности сети связи;

– нахождение удовлетворительного соотношения между достигаемым уровнем безопасности сети и безопасностью потребителей, использующих услуги связи;

– разработка и внедрение системы управления рисками и страхования ответственности операторов сети связи;

– обучение и переподготовка персонала сети связи в области обеспечения информационной безопасности программных средств сетей связи;

– оценка соответствия показателей безопасности программных средств сети связи требованиям задания на проектирование при проведении предварительных и приемочных испытаний и экспертизе проектной документации.

При этом возможно формулирование требования об обеспечении возможности независимой проверки результатов расчета безопасности программных средств сети связи, представленных разработчиком (поставщиком) согласно договорным обязательствам для проведения экспертизы.

Заключение. В данной работе выполнен комплексный анализ видов рисков, характерных для проектирования и строительства телекоммуникационных систем.

Показано, что факторы рисков могут привести не только к снижению интегральной экономической эффективности создаваемой системы связи, но и к ее полной нерентабельности. Поэтому предлагается расширить функции экспертной деятельности при анализе проектов в направлении осуществления количественного оценивания влияния имеющихся рисков на интегральные показатели этих проектов.

Проанализированы возможности применения известных методов риск-менеджмента при анализе и оценивании рисков проектирования и создания сетей связи, предложены методики и расчетные соотношения для учета неопределенностей условий реализации проектов и получения обоснованных экспертных выводов об уровне рисков.

В работе проанализированы возможности и показана необходимость учета как качественной информации о рисках сетей связи, так и количественных данных о рисках их проектирования и

функционирования. Результаты проведенного анализа позволяют выбрать наиболее подходящий для конкретного проекта метод оценивания рисков.

Проведен анализ рисков, обусловленных угрозами информационной безопасности сетей связи, в том числе безопасности программных средств. На основе анализа особенностей этапов проектирования и создания сети связи разработаны рекомендации по действиям на этапах жизненного цикла сети связи в направлении повышения проектного уровня безопасности технических и программных средств сети связи.

Сделан вывод о необходимости совершенствования правовой базы отрасли «Связь» в направлении создания и постоянной актуализации реестров рисков, установленных в ходе проектирования и строительства объектов связи.

Выполненная в данной работе апробация разработанных подходов и методик количественного оценивания рисков проекта телекоммуникационной системы показала возможность их реального применения как при проектировании, так и в практической деятельности экспертов, решающих задачи анализа уровня проектных разработок.

Предполагается, что применение предложенных рекомендаций и методического обеспечения приведет к улучшению интегральных показателей характеристик процессов проектирования и строительства телекоммуникационных систем.

По результатам данного анализа возможна разработка мер по оцениванию и минимизации предпринимательских и техногенных рисков сетей связи на этапах их проектирования, строительства и функционирования.

Полученные результаты могут быть использованы при создании научно-методической базы для применения методов экспертизы проектно-сметной документации с целью оценивания и снижения рисков проектирования и функционирования сетей связи.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 7 июля 2003 г. №126-ФЗ «О связи» (в ред.Федеральных законов от 22.08.2004 №122-ФЗ, с изм., внесенными Федеральными законами от 23.12.2003 №186-ФЗ, от 09.02.2007 №14-ФЗ).
2. Положение о составе разделов проектной документации и требованиях к их содержанию [утв. Постановлением правительства РФ от 16.02.08 г. №87].- М.: Информационно-правовой консорциум «Кодекс», 2008.
3. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.
4. ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты.
5. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем.
6. ГОСТ Р 51901.2-2005. Менеджмент риска. Системы менеджмента надежности.
7. ГОСТ Р 51901.4-2005. Менеджмент риска. Руководство по применению при проектировании.
8. ГОСТ Р 51901.5-2005. Менеджмент риска. Руководство по применению методов анализа надежности.
9. ГОСТ Р 51901.6-2005. Менеджмент риска. Программа повышения надежности.
10. ГОСТ Р 51901.11-2005. Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство.
11. ГОСТ Р 51901.13-2005. Менеджмент риска. Анализ дерева неисправностей.
12. ГОСТ Р 51901.14-2005. Менеджмент риска. Метод структурной схемы надежности.
13. ГОСТ Р 51901.15-2005. Менеджмент риска. Применение марковских методов.
14. ГОСТ Р 51901.16-2005. Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки.
15. ГОСТ Р МЭК 61160-2006. Менеджмент риска. Формальный анализ проекта.
16. ГОСТ Р ИСО 17666-2006. Менеджмент риска. Космические системы.
17. ГОСТ Р ИСО 15265-2006. Менеджмент риска. Основы стратегии оценки риска для предупреждения стресса и дискомфорта в термальных рабочих средах.
18. ГОСТ Р ИСО/МЭК 16085-2007. Менеджмент риска. Процессы жизненного цикла систем программного обеспечения.
19. ГОСТ Р 52806-2007. Менеджмент рисков проектов. Общие положения.
20. Федеральный закон «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений» №22-ФЗ от 02.01.2000 г.
21. Методические рекомендации по оценке эффективности инвестиционных проектов / Министерство экономики РФ, Министерство финансов РФ, Государственный комитет РФ по строительной, архитектурной и жилищной политике 21.06.1999 № ВК 477 [Электронный ресурс] // Информационно-правовая система «КонсультантПлюс». – М., 2006.
22. Шапкин А.С., Шапкин В.А. Теория риска и моделирование рисковых ситуаций: Учебник. 2-е изд. – М.: Издательско-торговая корпорация «Дашков и Ко», 2007. – 880 с.
23. Чернова Г.В., Кудрявцев А.А. Управление рисками: учебное пособие. – М.: Проспект, 2008. – 160 с.
24. Балдин К.В. Риск-менеджмент: Учебное пособие/ К.В. Балдин; – М.: М.: Эксмо, 2006. – 368 с.
25. Ступаков В.С., Токаренко Г.С. Риск-менеджмент. – М.: Финансы и статистика, 2007. – 288 с.
26. Черкесов Г.Н. Надежность аппаратно-программных комплексов. Учебное пособие. – СПб.: Питер, 2005. – 479 с.
27. Мельчаков А.П. К теории прогнозирования риска аварии объектов строительства// Вестник Южно-Уральского государственного университета. Серия «Строительство и архитектура». 2001. – Вып. 1.
28. Риск-менеджмент инвестиционного проекта/ под ред. М.В. Грачевой, А.Б. Секерина. – М.: ЮНИТИ-ДАНА, 2009. – 544 с.
29. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: примеры использования. – Рига: Зинатне, 1990. – 184 с.
30. Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий. – ФСТЭК России, 2005 г.
31. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд., стер. – М.: Издательский центр «Академия», 2008. – 336 с.
32. Цирлов В.Л. Основы информационной безопасности: краткий курс. –Ростов н/Д: Феникс, 2008. – 253 с.

УДК 004.72

ИНТЕГРАЦИЯ ОБРАЗЦОВ РАДИОЭЛЕКТРОННОГО ВООРУЖЕНИЯ НА ОСНОВЕ ИНФОРМАЦИОННОЙ ТРАНСПОРТНОЙ СЕТИ КОРАБЛЯ

Татарникова Татьяна Михайловна[1] Яготинцева Наталья Владимировна[2],
[1] Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
[2] Российский государственный гидрометеорологический университет,
Россия, Санкт-Петербург, Малоохтинский пр., д. 98,
e-mail: tm-tatarn@yandex.ru.

Аннотация: В статье рассматриваются современные задачи интеграции образцов радиоэлектронного вооружения с точки зрения обеспечения полноценного вхождения корабля в единое информационное пространство ВМФ.

Ключевые слова: *радиоэлектронное вооружение; интеграция; информационная инфраструктура корабля; локальная вычислительная сеть корабля; технология коммутации сегментов сети.*

TECHNOLOGY INFORMATION COMMUNICATION AND SECURITY

Tatarnikova Tatiana[1], Yagotinceva Natalia[2],
[1] Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2] Russian State Hydrometeorological University,
Russia, St. Petersburg, Malookhtinsky prospect, 98,
e-mail: tm-tatarn@yandex.ru.

Abstract: The paper considers the problem of integration of modern electronic equipment designs in terms of providing a full entry of ship into a single information space of the Russian NAVY.

Keywords: *radio-electronic equipmen; integration; information infrastructure ship's local area network of the ship; the technology switching network segments.*

Введение. Для решения задач навигации и кораблевождения, освещения обстановки корабли оснащаются многофункциональным радиоэлектронным вооружением (РЭВ).

В практике строительства и применения флота к радиоэлектронному вооружению, как правило, относят следующие классы РЭВ: радиолокационные комплексы и станции, средства связи, гидроакустические комплексы и станции, аппаратуру опознавания, комплексы радиоразведки, информационно-управляющие системы и другие средства, обеспечивающие преобразование и обработку электромагнитных (акустических) сигналов и данных.

Стремительный прогресс в области морской радиоэлектроники сделал корабельное РЭВ наиболее быстроразвивающимся наукоемким и дорогостоящим элементом корабля. Проблемы совершенствования РЭВ корабля приобретают особую значимость и актуальность в строительстве флота России XXI века, в основу которого положен принцип совершенствования качественных параметров образцов вооружения и военной техники [1],[2].

Цель статьи – охарактеризовать основные задачи и пути совершенствования РЭВ корабля, основанных на применении возможностей существующих базовых технологий и поддерживающих их технических и программных средств.

1. Архитектура образца РЭВ. Изучение функций, методов приема и обработки сигналов в комплексах, станциях и образцах РЭВ показало, что между устройствами различных классов РЭВ существуют тесные информационные взаимосвязи. Результаты работы одних из них являются исходными данными для других. Это обстоятельство позволяет утверждать, что существуют предпосылки для технической и информационной интеграции различных классов РЭВ корабля. Кроме того, исследования и анализ конкретных образцов РЭВ корабля показали, что существуют стандартные этапы обработки информации, а следовательно, любой образец РЭВ может быть описан шестью функциональными элементами (ФЭ).

ФЭ1: устройства, осуществляющие преобразование электромагнитной (акустической) энергии, как в случае излучения, так и приеме сигналов, или другими словами - антенны.

ФЭ2: устройства, осуществляющие прием, усиление, демодуляцию и декодирование сигналов – приемники.

ФЭ3: устройства, осуществляющие прием, усиление, модуляцию и передачу сигналов – передатчики.

ФЭ4: средства обработки сигналов и данных соответствующей прикладной платформой.

ФЭ5: средства визуализации, обеспечивающие динамическое отображение целей и их траекторий движения; документирование данных на карту и бумажный носитель; просмотр документов и статистическое отображение наиболее важных данных.

ФЭ6: устройства, обеспечивающие преобразование воздействий окружающей среды в электромагнитные сигналы – датчики.

В целом обобщенная архитектура образца РЭВ с прикладной платформой обработки приведена на рисунке1.

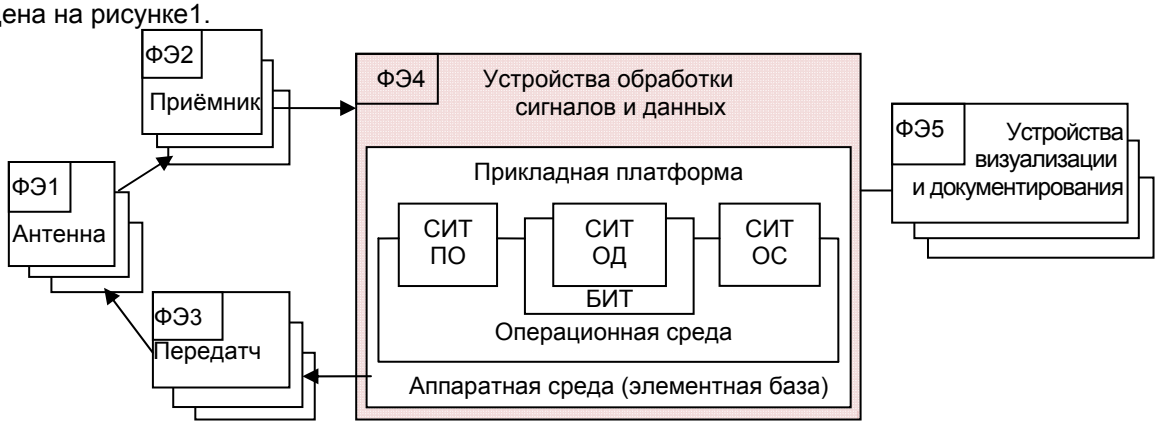


Рис. 1. Обобщенная архитектура образца РЭВ

СИТ ПО – Специализированная информационная технология протоколов обмена;
СИТ ОД – Специализированная информационная технология обработки данных;
СИТ ОС – Специализированная информационная технология обработки сигналов;
БИТ – Базовая информационная технология

СИТ ПО включает:	**СИТ ОС включает:**
– Поддержку протокола обмена по СНЧ, СДВ, СВ, КВ, УКВ, радиорелейным, космическим, гидроакустическим, проводным каналам. – Поддержку сетевых протоколов типа TCP/IP, ATM, X.25. – Поддержку стандартов защиты информации в каналах связи и сетях передачи данных.	– Обработку радиолокационных сигналов. – Обработку радиосигналов. – Обработку оптоэлектронных сигналов. – Обработку гидроакустических сигналов. – Оцифровка аналоговых сигналов.
СИТ ОД включает:	**БИТ включает:**
– Обработку координат. – Обработку ЭДЦ. – Прокладку маршрутов. – Учет целей. – Выработку данных стрельбы. – Визуализацию данных. – Классификацию целей. – Обработку результатов измерений. – Выработку рекомендаций по маневрированию, счислению пути. – Ведение журналов учета.	– Информационные технологии (ИТ) электронной почты. – ИТ документооборота. – ИТ СУБД. – ИТ ГИС. – Офисные ИТ. – Формирование, поиск и предоставление информационных ресурсов. – Защиту информационных ресурсов. – Электронные подписи. – Управление конфигурацией. – Сетевое планирование. – Санкционирование применения оружия.

2. Основные направления развития РЭВ корабля. В соответствии с рассмотренной архитектурой образца РЭВ можно сформулировать основные направления развития РЭВ корабля:

1. Развитие устройств преобразования электромагнитной (акустической) энергии во всех диапазонах электромагнитного спектра за счет применения новых материалов, форм построения и технологий производства.
2. Развитие устройств генерирования и приема электромагнитных сигналов во всех диапазонах электромагнитного спектра за счет применения новой элементной базой и более совершенных схем их построения.
3. Развитие методов и способов обработки электромагнитных и акустических сигналов.
4. Развитие средств и прикладных платформ обработки сигналов и данных.
5. Развитие средств визуализации данных на основе применения новых технологий отображения информации, мультимедийных форм ее представления, а также за счет использования новой элементной базы.
6. Интеграция образцов РЭВ в единую информационную инфраструктуру корабля с переходом к новой архитектуре их построения.

Направления 1-4 относятся к числу традиционных и хорошо освоенных. В направлении 5 наметились за последние годы существенные позитивные сдвиги.

Анализ исследований в этом направлении с учетом достижений последнего десятилетия в области создания эффективных средств обработки сигналов и данных показывает, что наибольший эффект в реализации возможностей базовых информационных технологий и поддерживающих их технических и программных средств может быть получен на пути интеграции образцов РЭВ в единую информационную инфраструктуру корабля. Таким образом, шестое направление развития РЭВ является наиболее перспективным.

Справедливость этого утверждения подтверждается тем, что сегодня на корабле отсутствуют:

– единое адресное пространство;

– прозрачный доступ, в соответствии с полномочиями должностных лиц к удаленным и обособленно хранящимся информационным ресурсам;

– средства, обеспечивающие реализацию мультимедийного трафика обмена информацией;

– унифицированная система панелей диалога для разнородных автоматизированных рабочих мест.

Поэтому перспективным направлением развития вооружения корабля сегодня считается интеграция образцов РЭВ в единую информационную инфраструктуру корабля с переходом к новой архитектуре их построения [3],[5],[6].

Суть нового подхода заключается:

– В интеграции образцов РЭВ не на основе парных связей, а на основе базовой информационной транспортной сети корабля.

– В обеспечении возможности подключения к базовой корабельной сети комплексов, станций различных типов РЭВ и функциональных элементов.

– Во введении в состав технической архитектуры нового элемента – комплекса серверов обработки сигналов и данных.

– В переходе от функционально-специализированных архитектур средств обработки сигналов и данных к распределенной сетевой обработке [4].

Техническая архитектурная модель информационной инфраструктуры корабля с учетом нового подхода представлена на рисунке 2 и представляет собой локальную вычислительную сеть (ЛВС) корабля с коммутацией сегментов [7].

Технология коммутации сегментов основана на отказе от использования разделяемых линий связи между всеми узлами сегмента и использовании коммутаторов, позволяющих одновременно передавать пакеты между всеми парами его портов [8].

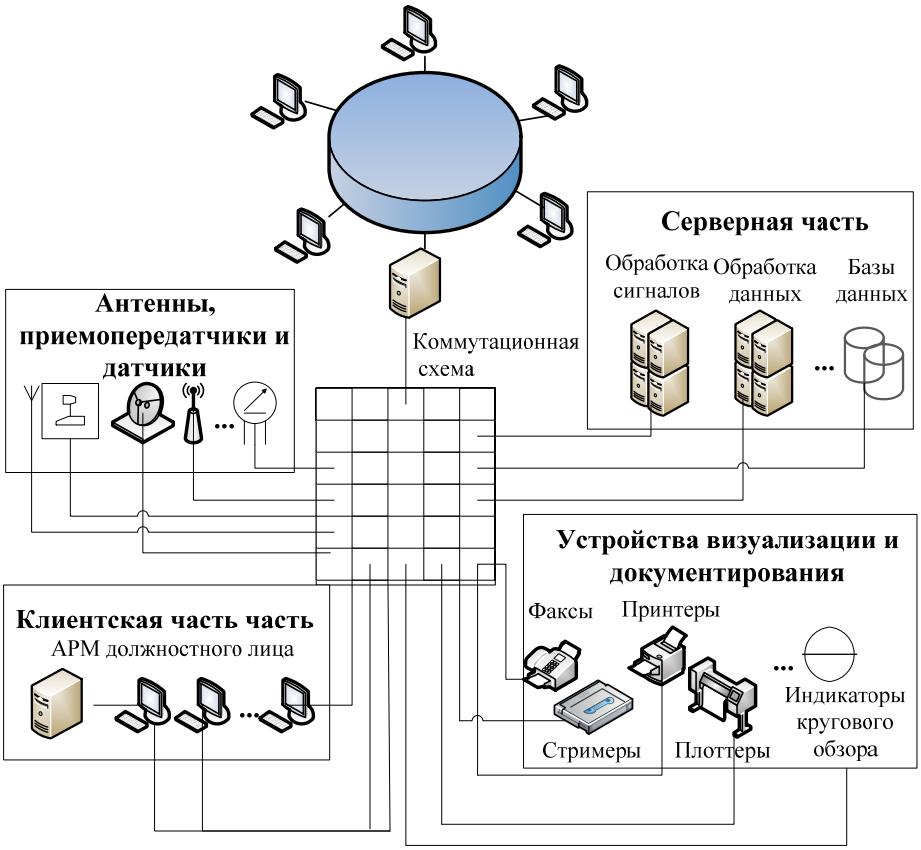


Рис.2. Архитектура информационной инфраструктуры корабля на основе базовой информационной транспортной сети

Заключение. Придание информационной инфраструктуре корабля новых качеств в смысле сетевой организации транспортировки информации и распределенной обработки сигналов и данных, может кардинально изменить информационный облик корабля [2],[3].

Локальная вычислительная сеть корабля позволит:

– исключить параллелизм в выполняемых функциях образцов РЭВ;
– сократить стоимость создания и эксплуатации РЭВ;
– повысить надежность, живучесть и ремонтопригодность образцов РЭВ.

СПИСОК ЛИТЕРАТУРЫ

1. Директоров Н.Ф., Катанович А.А. Современные системы внутрикорабельной связи. СПб.: Судостроение, 2001.
2. Воскресенский В.В., Доценко С.М., Чудаков О.Е. Информационное обеспечение управления и флот. СПб, Ника, 2002.
3. Чугреев О. С., Верзун Н. А. Управление структурой локальных информационных сетей // Сборник трудов международной конференции ICI&I'97. – СПб., 1997. С.248–250.
4. Татарникова Т.М., Яготинцева Н.В. Модель оценки характеристик локальной вычислительной сети корабля //Материалы международной конференции «Теоретические и прикладные проблемы науки и образования в 21-м веке», часть 5, Тамбов. С. 143-144.
5. Татарникова Т.М., Яготинцева Н.В. Характеристика проблемы интеграции образцов радиоэлектронного вооружения корабля//Ученные записки РГГМУ. 2012. №25. С. 156-162.
6. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени//Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4. С. 150-151
7. Татарникова Т.М., Шанти Й. Аналитическая модель коммутатора с общей памятью//Технические средства судовождения и связи на морских и внутренних водных путях. Международный межвузовский сборник научных трудов. СПб.: СПбГУВК. 2006. Выпуск 7. С. 141-146.
8. Миронов В.В., Головкин Ю.Б., Юсупова Н.И. Об автоматной модели динамической ситуации // Управление сложными техническими системами: межвузовский научный сборник. Уфа: УАИ. 1986. №9. С. 3-10.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ОТЗЫВ И ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ В РЕШЕТОЧНОЙ VLR-СХЕМЕ ГРУППОВОЙ ПОДПИСИ

Александрова Елена Борисовна, Кузнецова Екатерина Александровна,
Санкт-Петербургский государственный политехнический университет,
Россия, Санкт-Петербург, ул. Политехническая, д. 29
e-mail: kafedra@ibks.ftk.spbstu.ru.

Аннотация: В статье рассмотрены решение задачи ананимного подтверждения достоверности защиты информации в виде протокола групповой подписи, процедура отзыва права подписи и добавления пользователя в группу, отзыв, локальный для проверяющего (VLR).

Ключевые слова*: групповые подписи; отзыв, локальный для проверяющего; решетка.*

REVIEWS AND ADDING USERS TO THE VLR-LATTICE CHART GROUP SIGNATURE

Alexandrova Elena, Kuznetsova Ekaterina,
Saint Petersburg State Polytechnical University,
Russia, Saint-Petersburg, ul. Polytechnique, d. 29,
e-mail: kafedra@ibks.ftk.spbstu.ru.

Abstract: The article deals with the solution of anonymity is conferred validation of information security in the form of protocol group signature recall procedure of signature and add a user to a group, add to the local inspector (VLR)

Keywords: *group signature; verifier local revocation; grid.*

В ряде прикладных областей для защиты информации требуется анонимное подтверждение ее достоверности. Для решения этой задачи используются специальные схемы цифровой подписи, обеспечивающие анонимность подписывающего, − групповые подписи [1].

Важными составляющими протокола групповой подписи являются процедуры отзыва права подписи и добавления пользователя в группу. Наиболее эффективным вариантом отзыва является отзыв, локальный для проверяющего (verifier local revocation, VLR). В таких схемах сообщения, содержащие информацию об отозванных членских сертификатах, обрабатываются только проверяющими. Основным преимуществом VLR-схем групповой подписи является то, что выпускаемые записи отзыва никак не привязаны к используемым ключам. Тем самым они позволяют отзывать не право подписи у члена группы, как при отзыве с динамическим накоплением, а сами подписи, им сформированные.

Одной из перспективных альтернатив «традиционным» алгебраическим структурам, используемым для построения схем групповой подписи, являются решетки. Первая попытка интеграции решеток в механизм групповых подписей была предпринята в работе [2]. Протокол, построенный в целом по шаблонам схемы BMW, использует модель со случайным оракулом. Дальнейшее развитие данная схема получила в работе [3]. Основной особенностью этого протокола является малый размер цифровой подписи. Схема обеспечивает: анонимность (причем возможно обеспечение полной CCA-анонимности) и отслеживаемость.

Однако оба эти протокола не предоставляют достаточной функциональности, поскольку не обладают наиболее востребованными свойствами схем групповой подписи: возможностью отзыва подписи и добавления нового участника в группу без изменения существующих параметров криптосистемы. Поэтому основой данного исследования стал протокол [4]. Указанный протокол предоставляет возможность для организации необходимых функций. Кроме того, защита строится на задаче SIVP (short integer solution problem: для данной m-мерной решетки, образованной базисом, равномерно распределенным над (Z/qZ)^nxm, найти кратчайший вектор с p-нормой), в отличие от более ранних протоколов, безопасность которых основана на задаче LWE (learning with errors).

Основу схемы составляет интерактивный протокол, позволяющий предоставить проверяющему доказательство того, что подписывающий является сертифицированным членом группы (то есть владеет ключом подписи), и что ключ отсутствует в списке отозванных.

Для данного протокола механизм отзыва будет выглядеть следующим образом. Для секретного ключа каждого из пользователей рассмотрим первый блок x_0, соответствующий корню «дерева бонсай» (см., например, [5]) и положим маркер отзыва равным A_0*x_0 (mod q) из (Z/qZ)^n. При правильном выборе параметров значение маркера будет равномерно распределено над (Z/qZ)^n.

Пользователю предлагается вычислить значение функции c_0 по схеме обязательств COM [6] от случайного вектора r_0 из (Z/qZ)^m. Далее, в зависимости от целей проверяющего, пользователь передает либо значение r_0, либо r_0+x_0. В первом случае можно проверить честность вычисления c_0, во втором – содержится ли ключ пользователя в списке RL отозванных: для всех u_i из RL должно выполняться неравенство c_0 != COM(A_0(r_0+x_0) – u_i mod q).

Таким образом, если сертификат у пользователя отозван, то найдется такое i, что A_0*x_0 (mod q) = u_i. Процедура добавления пользователя в группу по новому идентификатору изменяет ключ подписи пользователя и ключ отзыва менеджера группы.

Модифицированная схема обладает свойствами «чужой» анонимности, отслеживаемостью, возможностью отзыва членства. В то же время является простой, поскольку основывается на доказательстве знания «все-в-одном» с использованием парадигмы Фиата-Шамира, и эффективной: для параметра безопасности n и числа пользователей N открытый ключ группы и подпись имеют длину порядка O(n^2 logN).

СПИСОК ЛИТЕРАТУРЫ

1. Chaum D., van Heyst E. Group signatures // Proceedings of Eurocrypt 1991, Springer-Verlag, Apr. 1991. P. 257–265
2. S.D.Gordon, J.Katz, V.Vaikuntanathan. A Group signature scheme from lattice assumptions // https://eprint.iacr.org/2011/ 060.pdf
3. F.Laguillaumie, A.Langlois, B.Libert, D.Stehle. Lattice-based group signatures with logarithmic signature size // http://eprint.iacr.org/2013/308.pdf
4. A.Langlois, S.Ling, K.Nguyen, H. Wang, Lattice-based group signature scheme with verifier-local revocation // Public Key Cryptography – PKC2014, Springer, 2014. LNCS. Vol. 8383. P. 345-361
5. D.Cash, D.Hofheinz, E.Kiltz, C.Peikert. Bonsai trees, or How to delegate a lattice basis // http://www.cc.gatech.edu/~cpeikert/pubs/bonsai.pdf
6. A. Kawachi, K. Tanaka, K. Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems // ASIACRYPT. Springer, 2008. LNCS. Vol. 5350. P. 372-389

УДК 004.05

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО: 20 ЛЕТ КОНЦЕПТУАЛЬНОГО И ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ

Алексеев А.В.[1], Воробьев В.И.[2],
[1]Россия, Санкт-Петербургский государственный морской технический университет,
Санкт-Петербург, ул. Лоцманская, д. 3,
[2]Россия, Санкт-Петербургский институт автоматизации и информатизации РАН,
199178, Санкт-Петербург, 14-линия ВО, д. 39,
e-mails: iapbgks@bk.ru, vvi@iias.spb.su

Аннотация: В статье выполнен анализ 20-летнего периода концептуального и технологического развития сил и средств ведения информационного противоборства от концепций информационных войн до современного их варианта в форме сетецентрических войн. Показано, что только на основе широкомасштабных, хорошо скоординированных процессов информационного противоборства с использованием возможностей современных информационных технологий можно фактически парализовать систему управления силами и оружием противника без нанесения ему невосполнимых ресурсных потерь. Сформулированы проблемы и реальные пути преодоления отставания в области информационного противоборства.

Ключевые слова: *информационная война, сетецентрическое противоборство, технологическое превосходство, ликвидация преимуществ.*

INFORMATION CONFRONTATION: 20 YEARS OF CONCEPTUAL AND TECHNOLOGICAL DEVELOPMENT

Anatoliy Alekseev[1], Vladimir Vorobiev[2],
[1] The St. Petersburg State Marine Technical University,
Russia, St. Petersburg, Lozman str. 5,
[2] Russia, Saint-Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14 Line,39
e-mails: iapbgks@bk.ru, vvi@iias.spb.su

Abstract: The analysis of the 20 year period of conceptual and technological development of forces and means of conducting information warfare from concepts of information warfare to their modern version in the form of network-centric warfare is presented in the paper. It is shown that only through large-scale, well-coordinated processes of information warfare with the use of modern information technologies the adversary's system of control of forces and weapons can be actually paralyzed without inflicting irreparable resource losses. Problems are formulated and realistic ways to overcome the backlog in the field of information confrontation are proposed.

Keywords: *information warfare, network-centric confrontation, technological superiority, the elimination of benefits.*

Введение. Понятия «информационное противоборство» (ИП), «информационная война», «ведение боевых действий в едином информационно-коммуникационном пространстве» или в современном варианте «сетецентрическая война» рассматриваются сегодня, как система боевых противоборств с применением воинских формирований, как модель своеобразных устройств, подключенных к единой сети [1], [2].

В этом, собственно, и проявляется эффект синергизма ИП (2+2=5), когда целое представляет нечто большее, чем сумма его частей. Этот системный (синэргетический, эмерджентный) эффект от совместного действия объединенных в сеть средств вооруженной борьбы по совокупному результату превышает сумму эффектов от применения тех же средств ведения вооруженной борьбы по отдельности.

Для достижения эффекта синергизма ИП необходима, прежде всего, совершенная «цифровизация» самой системы управления [1]. Но это только начало пути, потому что неотъемлемым условием реализации новой концепции становится развертывание компьютерных сетей и обеспечивающих информационных технологий, то есть современных аппаратных и программных средств, средств обеспечения автоматизации процессов подготовки и принятия тактических, оперативно-тактических, оперативных и оперативно-стратегических решений, хранения, обработки и доведения информации и многого другого. Причиной постановки данной темы анализа послужил 20-летний период, прошедший с первой постановки авторами проблемы анализа возможностей, развития технологий и концепций ведения информационных войн в 1995 г. в процессе подготовки к V Санкт-Петербургской международной конференции «Региональная информатика-96» [3]. Основные положения сформулированной ранее концепции ведения информационных войн приведены на рисунке 1.

Актуальность. В порядке анализа тенденций концептуального и технологического развития ведения информационного противоборства за прошедший 20-летний период авторам представляется весьма актуальным рассмотреть динамику реализации ранее сформулированных и перспективу развития новых принципов и технологических возможностей.

Состояние проблемы. В настоящее время известны следующие основные направлений технологического развития перспективных комплексов автоматизации военного управления:

– расширение спектра и перечня функциональных возможностей автоматизации управления;

– совершенствование архитектуры автоматизированных систем управления для реализации принципов распределенной обработки данных и ее согласование с общей структурой управления;

– стандартизация и унификация оборудования, информационного и программного обеспечения.

В этих условиях качественное повышение уровня информационно-аналитичес-кого и интеллектуального обеспечения боевых действий становится определяющим фактором достижения стратегического и оперативно-тактического превосходства над противником.

Так, известные положения современной концепции «сетецентрическая война» предполагает качественно новый уровень взаимодействия сил и средств и характеризующийся следующими основными особенностями [4], [5]:

– значительным возрастанием объемов анализируемой и циркулирующей информации, а также повышением качества и критичностью восприятия текущей обстановки;

– улучшением качества взаимодействия разнородных сил, повышением степени согласованности и целенаправленности их действий, а также оперативности управления;

– повышением эффективности применения сил и средств, значительным повышением динамизма и масштаба проводимых операций и перемещаемых военных контингентов.

– Модель сетецентрической войны (сетецентрического противоборства (СЦП), показана на рисунке 2.

– Как показывает анализ ряда источников [2], [5], [6], модель представляет собой систему, состоящую из трех решеток-подсистем в соответствии с рисунком 3: сенсорной, информационной, боевой.

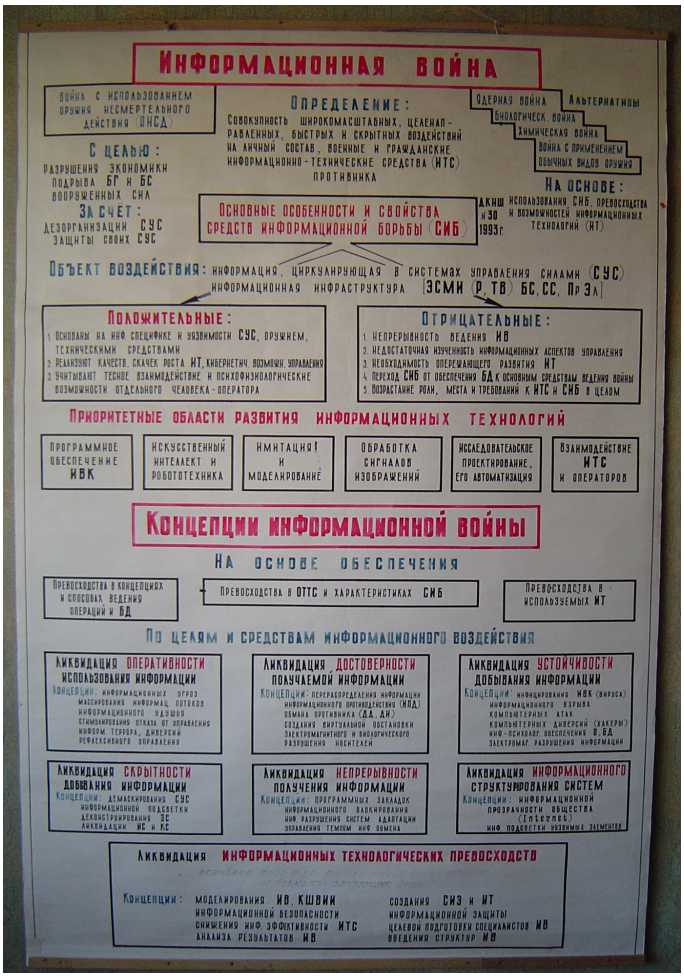


Рис.1. Концепции ИВ (вариант, 1995 г.)

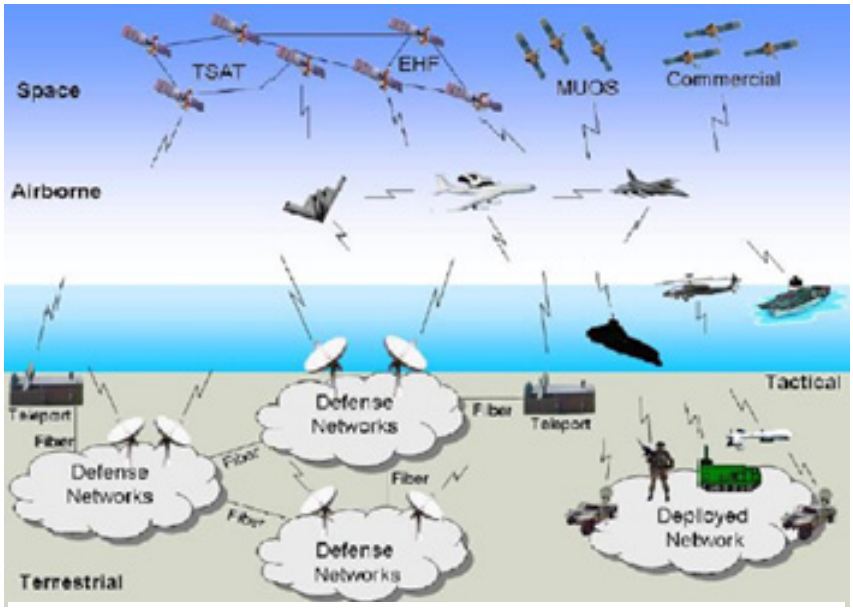


Рис. 2. Система связи для управления при проведении сетецентрических войн

Основу этой системы составляет информационная решетка, на которую накладываются взаимно пересекающиеся сенсорная и боевая решетки. Элементами сенсорной системы являются «сенсоры» (средства разведки), а элементами боевой решетки – «средства поражения». Эти две группы элементов объединяются воедино техническими средствами органов управления и командования.

Информационное превосходство в ходе ИП (СЦП) – это не передача в большом количестве информации к элементам боевого построения, а достижение соответствующего обстановке

осознания и понимания ситуации в пространстве информационного противоборства. Более точного уяснения своих преимуществ и недостатков противника.

Рис. 3. Принцип ведения сетецентрической войны

Это – способность сформировать замысел действий, в котором эти преимущества будут в максимальной степени реализованы, а недостатки противника использованы в своих целях. Это – опережающее принятие и незамедлительное доведение до подчиненных и взаимодействующих сил и средств решений, полностью адекватных сложившейся обстановке. Более того, непрерывный контроль их исполнения.

Сторонники сетецентрических концепций утверждают [1], что формирование единого информационного пространства, позволяющего каждому участнику боевых действий иметь точные данные о ситуационной осведомленности, повышает уровень взаимодействия, самосинхронизации, скорость управления подчиненными силами, в конечном счете, и боевые возможности формирований.

В зависимости от выбора сетевой архитектуры и ее типа такими устройствами могут быть корабли, самолеты, средства поражения, управления, связи, разведки и наблюдения, группа военнослужащих или отдельные солдаты, а также комбинация и тех, и других. В этом случае возможности боевых формирований определяются не столько индивидуальными тактико-техническими характеристиками отдельных образцов ВВТ, сколько возможностями всей группы подключенных к сети средств как единого целого.

Проблемы совершенствования технологий ИП. В виду особенностей ИП (современной его концепции в форме СЦП), а именно, создания удаленного управления от места события, необходима, прежде всего, подробная и адекватная картина представления информации, учитывающая особенности восприятия информации операторами и лицами, принимающими решения (ЛПР), а также для возможности принятия ЛПР своевременного решения. Поэтому специфическими для задач ИП требованиями к силам и средствам его обеспечения могут быть названы, прежде всего:

– превосходство в концепциях и способах ведения информационных операций и информационно-боевых действиях, как отмечалось еще 20 лет назад (рисунок 1) на основе обеспечения превосходства в оперативно-тактико-технических свойствах (ОТТС) и характеристиках используемых сил и средств ведения ИП (СИП), а также превосходства в целом используемых информационных технологий (ИТ). Решение этой системной задачи предусматривает разработку и приоритетную реализацию соответствующей национальной программы;

– превосходство в целях и средствах ИП (рисунок 1) на основе соответствующих сетевых сил и средств управления и связи, разведки, средств поражения, личного состава и обеспечения, причем, приоритетным и первостепенным направлением, как показывает опыт, следует считать совершенствование форм и методов организационного управления с максимальным обеспечением прозрачности информационного поля управления на основе современных технологий открытой (прозрачной) оптимизации проектных и управленческих (для ЛПР) решений (ПУР). При этом, достигаемыми целями ИП должны быть:

– ликвидация оперативности использования информации потенциальным противником (ПП) *на основе концепций* массирования информационных потоков, информационного удушья, стимулирования отказа от управления, информационного психоза, информационного террора и диверсий, рефлексивного управления и др.;

– ликвидация достоверности получаемой ПП информации на основе концепций обмана ПП, перераспределения информации, создания многовариантной виртуальной обстановки, электромагнитного, биологического разрушения носителей и др.;

– ликвидация устойчивости добывания ПП информации *на основе концепций* информационного инфицирования, информационных взрывов, компьютерных диверсий, информационно-психологического обеспечения различных видов ИП и др.;

– ликвидация скрытности добывания и использования информации ПП *на основе концепций* информационной подсветки, демаскирования, деструктивных действий и др.;

– ликвидация непрерывности получения информации ПП *на основе концепций* информационного блокирования, активации информационных закладок, информационного разрушения систем адаптации, управления темпом информационного обмена и др.;

– ликвидации информационного структурирования систем ПП *на основе концепций* информационного вскрытия (подсказки) уязвимых элементов, управления информационной прозрачностью общества и сред взаимодействия и др.;

– превосходство в средствах автоматизированной (преимущественно – автоматической) многомерной комплексной визуализации и обработки информации (МКВОИ). Именно многомерность представления информации ЛПР позволяет, с одной стороны, отображать весь «огромный» массив данных, поступающий на автоматизированное рабочее место (АРМ) ЛПР, а, с другой стороны, максимально полно учитывать современные технологические возможности, аспекты и особенности средств в «комфортном» сопряжении с психофизиологическими возможностями ЛПР;

– превосходство в силах и средствах защиты информационных ресурсов ведения ИП и, в первую очередь, верхних степеней защищенности информации (критической информации). Как по традиционным критериям конфиденциальности, доступности, целостности, так и по основным критериям управления силами и средствами и свойствам используемой информации – её оперативности (своевременности), достоверности, устойчивости, скрытности, непрерывности, а также интегральных её критериев – ценности информации и безизбыточности. В этой связи, особое значение приобретают средства и технологии обеспечения информационной маскировки и дезинформации противника, как специфических форм оперативного (тактического, оперативно-тактического, оперативно-стратегического, стратегического) искусства ведения ИП (СЦП);

– превосходство в силах и средствах информационных вторжений с совершенным организационно-техническим арсеналом ведения повседневных информационно-боевых действий, информационных атак, информационных операций, информационных сражений и других форм. При этом весьма значимым следует считать непрерывное накопление опыта ИП, его актуализации, в том числе в процессе специальной подготовки, учебно-тренировочной работы и проведения комплексных учений по ИП;

– превосходство в теоретическом и научно-методическом обеспечении ведения ИП, подготовки и переподготовки специальных кадров, как принято сегодня их называть – кибервоинов. Особое значение в этом контексте должно принадлежать проведению специализированных научно-исследовательских и опытно-конструкторских работ, обеспечивающих соответствующие приоритеты развития. В том числе на базе системно-аналитических обобщений опыта проведения различных видов и форм ИП в ходе международных конфликтов и войн последнего периода – Египет, Фолкленды, Югославия, Украина [7], Ирак, Афганистан, Ливия, Сирия и других.

Конечно, поставленные руководством РФ национальные задачи по обеспечению конкурентной способности и импортозамещаемости продукции, включая информационно-коммуникационные средства, только подчеркивают и должны обеспечить реализацию названных требований, причем, в обозримом ближайшем будущем.

Это позволит реально перейти от Доктрины информационной безопасности (12.09.2000) и национальной проблемы отставания в информационно-технологическом развитии к реализации национальной Концепции СЦП в любых по сложности эрготехнических системах (ЭТС). Так, конверсионным вариантом подобных боевых систем могут быть близкие по структуре и функциональному составу системы типа «Безопасный большой Город – Область – Регион» [9]. Одним из их ключевых элементов также должны быть методы организационного управления с максимальным обеспечением прозрачности информационного поля управления на основе технологий открытой (прозрачной) оптимизации проектных и управленческих решений, а по сути – реализации «принципа гармонизации управления» с согласованием целевых векторов всех элементов сложных ЭТС. При этом, используемые в составе ЭТС автоматизированные системы управления в защищенном исполнении (АСЗИ) должны быть полнофункциональными в части структуры и состава средств и подсистемы комплексной защиты информации (СКЗИ, рисунок 6), так и подсистемы информационного противоборства. Причем, как известно, качество используемых средств должно реально обеспечиваться системой сертификации соответствия, а в перспективе и системы сертификации качества, например, типа [10].

Тенденции развития технологий и средств ИП. Сопоставляя данные [3] и тенденции их развития, по мнению авторов, могут быть сформулированы следующие основные положения:

1. Развитие технологий ИП в отмеченный 20-летний период, бесспорно, характеризуется особой интенсивностью, должным вниманием, значительным объемом выделенных средств,

достижением определенных теоретических и практических результатов и, можно полагать, созданием достаточных условий для перспективного развития.

2. Среди направлений, в которых достигнуто определенное превосходство над потенциальным (возможным) противником следует выделить технологии защиты от вредоносных кодов, в том числе разрабатываемые компанией «Лаборатория Касперского» и некоторые другие специальные технологии.

3. Вместе с тем, наращивание требований, сложности решаемых задач и созданных технических регламентов приводит в условиях снижения сроков морального старения средств к определенному отставанию оснащенности информационных сетей и соответствующим уязвимостям безопасности.

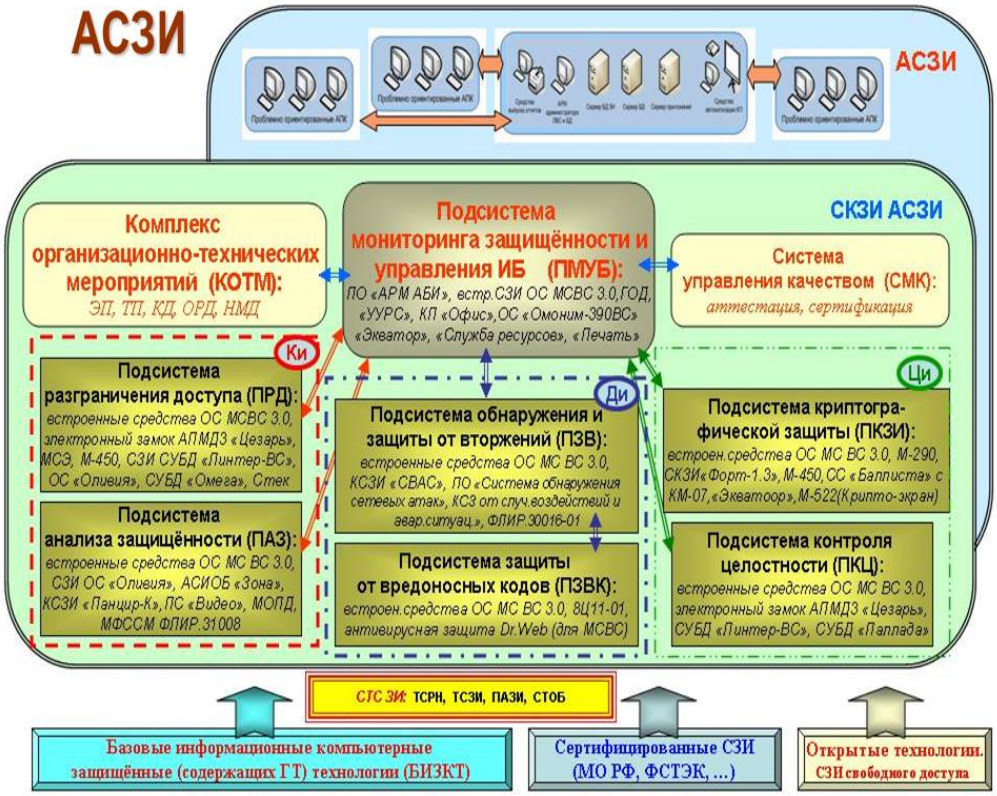


Рис. 6. Типовой состав и структура СКЗИ в составе АСЗИ

4. В этих условиях имеет место тенденция переоценки в ряде случаев угроз безопасности и недооценки возможности ведения активного и результативного информационного противоборства (рисунок 7).

Рис. 7. Анализ тенденций переоценки концепций ИП, угроз и уязвимостей

5. С другой стороны, редкий и избирательный характер инцидентов с реальными случаями информационных вторжений (атак) в условиях мирного времени, а также в условиях недостаточной оснащенности средствами мониторинга вторжений привел по существу к тенденции недооценки важности комплексного решения задач обеспечения защищенности информационных ресурсов и соответствующего выделения финансовых ресурсов. Это существенно снижает готовность сетей к работе в условиях возможного ИП (СЦП).

6. Среди актуальных направлений технологического развития, прежде всего, следует выделить наряду со сформулированными выше требованиями и результатами 20-летнего периода развития также:

– необходимость развития средств мониторинга и управления ИП в реальном масштабе времени с полномасштабными подсистемами информационно-аналитической и интеллектуальной поддержки операторов и руководящего состава *на основе* совершенствования технологий искусственного интеллекта и робототехники (рисунок 1).

– необходимость развития систем автоматического управления защищенностью сетей с алгоритмами адаптивного и самоорганизующегося управления с широкомасштабным использованием технологий прогнозирования развития обстановки и имитационного моделирования.

– неоправданное расширение номенклатуры разрабатываемых средств при одновременном их функциональном перенасыщении, что может быть интерпретировано как несовершенство технологий исследовательского проектирования (рисунок 1) и проектного управления. Это привело к расширению парка (более 3000) сертифицированных средств и снижению срока их жизненного цикла.

– недостаточное внимание уделяется развитию методологии квалиметрической оценки качества используемых средств и систем, включая использование агрегированных показателей качества, в том числе при оценке уровней конкурентной способности и управления процессами технологического развития (рисунок 1).

– необходимость применения методов анализа веб-контента для обнаружения злонамеренной деятельности в информационно-коммуникационных сетях. Анализ контента сайтов, связанных с терроризмом и построение «профиля» террориста используется для обнаружения в режиме реального времени лиц, подозрительных на предмет вовлеченности в террористическую деятельность.

Заключение. Выполненный ретроспективный анализ 20-летнего периода развития концепций и технологий информационного противоборства от концепций информационных войн (в том числе объявленной в известной сегодня Директиве объединенного командования начальников штабов НАТО № 30, 1993 г.) до концепций сетецентрических войн показывает все возрастающее значение информационного противоборства и его возможностей, а также признаки продолжающего отставания в этой области. Требует неотложного решения комплекс методических вопросов оценки конкурентной способности и импортозамещения средств ИП с переходом к технологиям сертификации соответствия качества. Для обеспечения паритета в области анализа веб-контента с целью обнаружения террористических угроз необходимы интенсивные научные и экспериментальные исследования с применением современных информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. От цифровизации к сетецентризму. – http://ss.lg.ua/node/578 от 29.07.2010
2. Мейчик Е. Р. Состояние и перспективы развития военной связи в Российской Федерации. http://www.mil.ru/info/53270/53288/index.shtml от 29.07.10.
3. Алексеев А.В., Кириллов Н.П., Тарасюк Ю.Ф. Информационная война: актуальность, возможности и концепции //Тез. докл.5 Санкт-Петербургской международной конференции «Региональная информатика-96», 13-16.05.1996, секция 4. - С-Пб.: СПИИРАН, 1996, часть 1. С.98 (исходный вариант – 10729, 1995, 1318).
4. Алексеев А.В., Орлов К.М. Возможности перспективных систем визуализации информации и поддержки принятия решений при проведении специальных атак и операций. – Петродворец, 2011, 1725, с.35-41.
5. Попов И.М. Сетецентрическая война. 2009. http://www.milresource.ru/NCW.html
6. Независимое военное обозрение http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html от 29.07.10.
7. Подберезкин А.И. Украина как частный пример ведения сетецентрической войны против России – Экспертный союз, 2015, № 16, с. 42–45.
8. Попов И.М. Война это мир: невоенные аспекты обеспечения безопасности государства, 2014 – http//: Eurasian-defence.ru/node/30886.
9. Алексеев А.В. Оптимизация проектных и управленческих решений при комплексном обеспечении безопасности большого города // Безопасность большого города / Сб. ст. под ред. Э.И.Слепяна. – С.-Петербург: Издательство Сергея Ходова, 2007, с. 400-418.
10. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор». Спб., 7-9.10.2014 – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. – 624 с. (С. 29–34).
11. Морская радиоэлектроника: Краткий справочник / Под ред. В.А. Кравченко. – СПб.: Политехника, 2002, – 270 с.
12. Алексеев А.В., Соколов Б.В. Теория информации: эволюция взглядов и подходов, современные проблемы и возможные пути развития /Проблемы информатизации - М.: РАН и Минпромнауки и технологий РФ, 2001, в.3, с.26–29.
13. Алексеев А.В. Эмерджентный анализ комплексного использования и защиты информации при оптимизации морских информационно-управляющих систем / IX междунар. конф. «Региональная информатика - 2002». Ч.1. – СПб., 2004, с. 58.

УДК 004.05

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ОБЛАЧНЫХ СЕРВИСОВ

Афанасьев Сергей Владимирович,
Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14-я линия ВО, д. 39,
e-mails: serg@sqlab.spb.su.

Аннотация: Облачная модель должна обеспечивать высокую степень готовности и безопасности вычислительных ресурсов в облаке. В статье исследовалась релевантная таксономия данных и сервисов в облачных вычислениях в части инфраструктуры как сервис IaaS и платформы как сервис PaaS, на основе онтологического описания таксономии доступа к данным и сервисам (доступность).

Ключевые слова*: облачные вычисления; инфраструктура; платформа; онтология.*

ONTOLOGICAL APROACH TO DEFINE CLOUD SRVICES

Afanasyev Sergey Vladimirovich,
The Saint-Petersburg Insitutete for Informatics and Automation RAS,
SPIIRAS, Russia, Saint-Petersburg, 14 Linia 39.
e-mails: serg@sqlab.spb.su.

Abstract: Cloud computing model should be adapted for high readiness and security of computational resources cloud. In this paper there were investigated relevant taxonomy of data and services in cloud computing in part of IaaS and PaaS on the base of ontology description of taxonomy to data and service.

Keywords: *cloud computing; infrastructure; platform; ontology.*

Введение. Облачные технологии разработаны с целью обеспечить работу и защиту инфраструктуры на всех уровнях и предоставляют возможности по улучшению перемещения, обработки и защиты данных в облаке.

Облачные вычисления – это использование компьютерных технологий, посредством которых динамически масштабируемые и виртуализируемые ресурсы обеспечиваются как обслуживание в сети Интернет. Облачные технологии применяются для решения ресурсоемких задач при сравнительно небольших мощностях терминальных устройств таких как персональные компьютеры, мобильные телефоны, интернет-планшеты. Данный метод позволяет значительно расширить вычислительные и иные возможности за счёт использования удаленного сервера, предоставленного владельцем за умеренную плату.

По мнению ведущих специалистов провайдеров, облако больше не раскладывается на четко определенные слои. В будущем многие приложения будут собирать разные сервисы и большие объемы данных из разных мест и совмещать их воедино. Здесь необходимо мета описание (семантическое или онтологический подход) данных и сервисов в различных облаках необходимо для выбора релевантных сервисов (таких как инфраструктура, платформы, объемы памяти и т.д.) и различных разрозненных источников данных. Пользователи перемещают и используют данные в облачных структурах. Здесь и возникает проблема быстрого и релевантного поиска данных и сервисов.

Компьютерное имитационное моделирование порождает громадные объемы данных, для анализа и организации которых требуются новые методы и технологии. Каждый год объемы данных почти удваиваются. Для анализа этих данных с целью нахождения тонких эффектов, упущенных в предыдущих исследованиях, требуются алгоритмы, которые одновременно могут работать с огромными наборами данных и обнаруживать при этом очень тонкие эффекты.

Онтологический подход определения пути к облачным сервисам. Онтологическое описание дает возможность автоматически строить структуру и таксономию данных и сервисов в вычислительных облаках и для больших данных из различных источников в различных форматах интегрировать данные на основе онтологий. Использование языка онтологий (Web Ontology Language, OWL) и языка запросов SPARQL позволит освободить пользователя от необходимости отбирать источники данных, в которых находится интересующая информация и осуществлять интеграцию данных на основе онтологий.

На данный момент отсутствует механизм поиска и обнаружения различных типов облаков. Поиск подходящих облачных услуг осуществляется потребителями вручную, поскольку, несмотря на существование многочисленных поисковиков предоставляемые ими результаты могут не содержать релевантных веб-страниц, удовлетворяющих исходным требованиям потребителя к сервису. Кроме того, просмотр всех результатов требует немало времени. Поисковые машины Google, MSN и др. – это эффективные инструменты поиска по запросу, но они не предназначены для определения связей

между облачными сервисами различных типов и нахождения, наиболее подходящих с точки зрения требований потребителя.

Следовательно, система обнаружения облачных сервисов как никогда актуальна. Она использует известные поисковые машины на начальных шагах для сбора информации о веб-сайтах облачных услуг. А затем, консультируется с облачной онтологией и распознает наиболее подходящие сервисы из списка всех предложенных [1]. Онтологическое описание позволит автоматически строить структуру и таксономию данных и сервисов в вычислительных облаках. Онтологический подход обеспечивает мета информацией, которая описывает семантику данных и сервисов, что обеспечивает взаимоотношения между человеком и вычислительными агентами. Основными компонентами онтологии являются: «классы или понятия», «отношения», «функции», «аксиомы». Онтология содержит набор понятий и связей между ними и может быть использована для извлечения информации для удовлетворения пользовательских запросов [2].

В облачных вычислениях облака обычно подразделяются на три различных уровня: Инфраструктура как сервис (IaaS), платформа как сервис (PaaS) и программное обеспечение как сервис (SaS).

IaaS включает «железо», ПО и оборудование для предоставления прикладных программных сред с основанной на использовании прайс-модель ресурсов.

PaaS предоставляет высокоуровневую встраиваемую среду построения, тестирования и размещения пользовательских приложений. В общем случае разработчики должны соблюдать некоторые ограничения, касающиеся типа ПО, которое они создают, чтобы выполнялось свойство масштабируемости встроенных приложений.

SaaS предоставляет специальное программное обеспечение (ПО), к которому у потребителя имеется удаленный доступ через Интернет с помощью основанной на использовании прайс-модели ресурсов.

В соответствии с требованиями и типами онтологического описания IaaS (Infrastructure as a Service) на рисунке 1 приведены три основных слоя (типа) онтологии и компонент инфраструктуры, которые требуют подробного онтологического описания в соответствии с вышеуказанными требованиями.

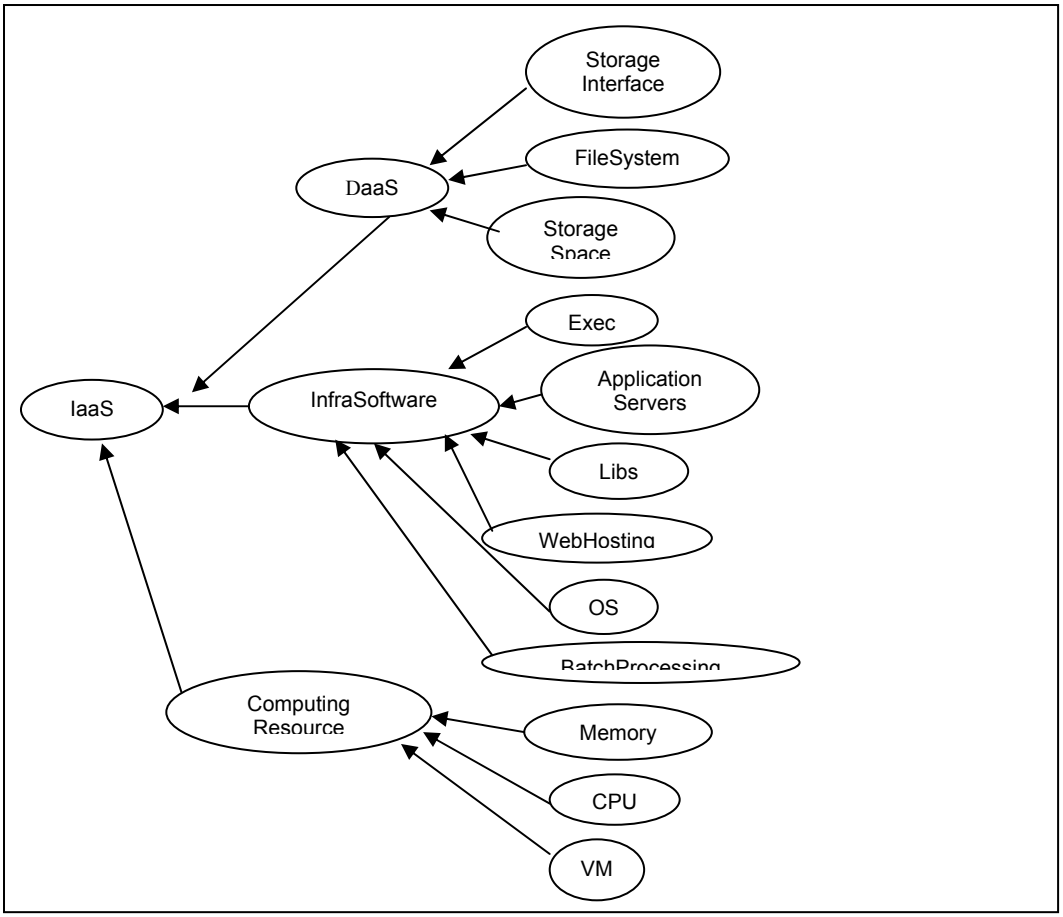


Рис. 1. Облачная онтология: IaaS

На рисунке 2 приведены основные слои (типы) онтологии и компонент платформ PaaS (Platform as a Service), которые также требуют подробного онтологического описания.

Для остальных сервисов таких, как SaaS, Compute as a Service, Storage as a Service и д.т. также необходимо онтологическое описание компонент и таксономии, что приведет к требуемому, релевантному «виртуальному облаку», состоящему из разных компонентов различных провайдеров вычислительных облаков [3].

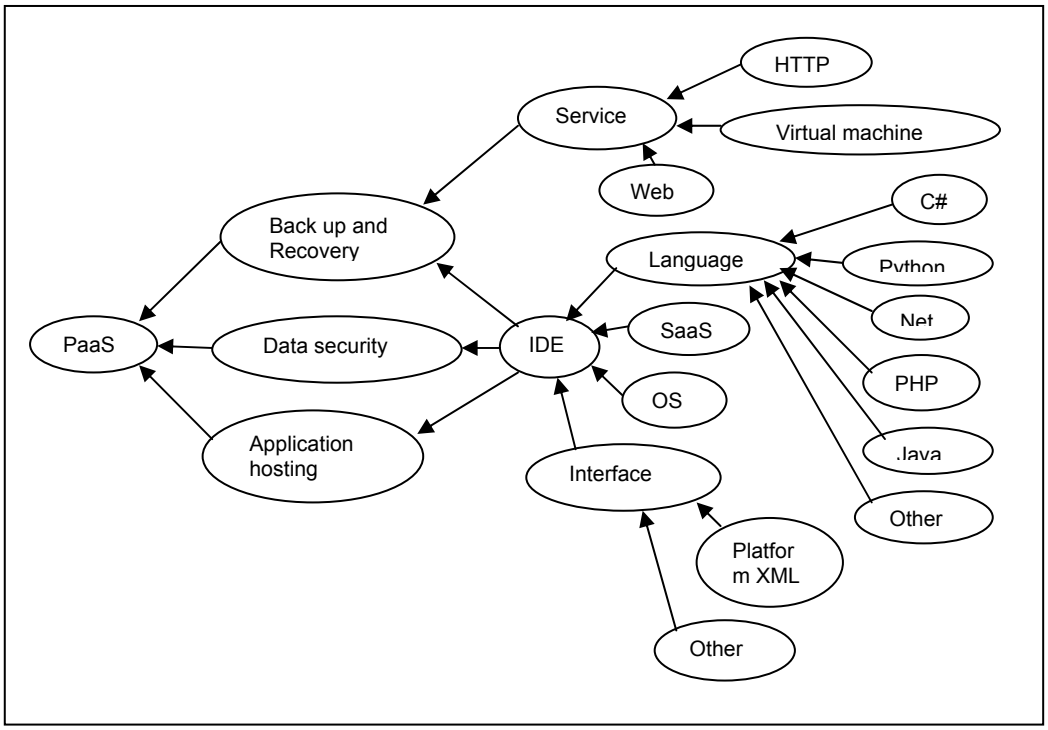


Рис. 2. Облачная онтология: PaaS

Заключение. Облачная онтология здесь представляет отношения между облачными сервисами с целью облегчить процесс поиска облачных понятий. В их число включены понятия облачных сервисов и данных, задействованных в данный момент, а также многих других, которые предполагается использовать в ближайшем будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Kwang M.S., «Toward an ontology-enhanced information filtering agent» in ACM SIGMOD Rec., vol. 33, Mar. 2004, pp. 95–100.
2. Taekgyeong H, Kwang M.S. An Ontology-enhanced Cloud Service Discovery System. Proceedings of the International Multiconference of Engineers and Computer Scientists 2010, v.I, IMECS 2010, March 17–19, 2010, Hong Kong.
3. Афанасьев С.В. Облачные сервисы, онтологическое моделирование таксономии. Тр. СПИИРАН, №4 (23), 2012, С. 392–399.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИОЛОГИЧЕСКИХ СИСТЕМАХ

Блюм Владислав Станиславович,
Санкт-Петербургский институт информатики и автоматизации РАН,
СПИИРАН, Россия, Санкт-Петербург, 14-я линия ВО, д. 39,
e-mails: vlad@blum.spb.su

Аннотация: Статья посвящена анализу иммунной системы человека, как системы информационной безопасности. В сложной биологической системе каждая клетка обладает признаком принадлежности данной системе. Этот признак доступен для контроля со стороны иммунной системы. Каждая клетка (структурно-функциональный элемент) может быть восстановлен либо из стволовой клетки, либо путем самокопирования (деления клеток). Каждая клетка лояльна к системе информационной безопасности, то есть, выдаёт сообщение о нарушении своей структуры и исполняемых функций, либо запускает процедуру апоптоза. В сложной биологической системе реализуется более одного способа удаления вторжений.

Ключевые слова: *Информационная безопасность; иммунная система; иммунный ответ.*

FEATURES INFORMATION SECURITY BIOLOGICAL SYSTEMS

Blum Vlad,
The St. Petersburg, SPIIRAS,
Russia, St. Petersburg, 14 line, 39,
e-mails: vlad@blum.spb.su

Abstract: The article analyzes the human immune system, as a system of information security. In a complex biological system, each cell has the sign of identity of this system. This feature is available for the control of the immune system. Each cell (structural and functional element) can be recovered either from the stem cells, either by copying (cell division). Each cell is loyal to the system, information security, ie, displays a message about the violation of its structure and executable functions or triggers apoptosis procedure. In a complex biological system is implemented more than one way to remove the intruders.

Keywords: *Information security; the immune system; the immune response.*

Введение. Поиск эффективных алгоритмов и способов организации данных для решения задач информационной безопасности проводится, в частности, в рамках научно-технического направления – иммунокомпьютинг [16,17,18]. Математические формализмы и алгоритмы иммунокомпьютинга опираются на современные знания о работе иммунной системы позвоночных и учитывают ее особенности. Анализу особенностей процесса устранения вторжений в организме позвоночного посвящена настоящая статья.

Есть основания считать, что иммунная система живого организма является наилучшим из известных образцов систем информационной безопасности, учитывая необычайную структурную и функциональную сложности объекта защиты.

В процессе эволюции живых существ возникли многоклеточные организмы. По мере усложнения их строения происходила специализация функций разных клеток и состоящих из них органов: пищеварения, дыхания и других. На определенном этапе эволюции в многоклеточном организме появились клетки, призванные защищать организм от опасных для него вторжений. Постепенно сформировалась особая система органов и клеток, обеспечивающих защиту (иммунитет) организма от вторжений, которая получила название иммунной системы. Клетки, входящие в состав иммунной системы, были названы иммунокомпетентными.

Отметим, что объект, называемый иммунной системой присутствует только у позвоночных животный. Наибольший интерес, безусловно, представляет иммунная система человека.

Иммунная система (от лат. Immunitas – освобождение) – это система организма, которая распознает, перерабатывает и устраняет чужеродные тела и вещества. В результате непрерывного выполнения функций распознавания, переработки и устранения чужеродных тел и веществ организм обладает замечательным свойством – иммунитетом.

Рассмотрим особенности иммунной системы человека как системы информационной безопасности всего организма и каждой его клетки. То есть попытаемся ответить на вопросы, как в биологической системе решаются задачи:

– обеспечения целостности информации, т.е. предотвращения несанкционированной записи информации,

– обеспечения конфиденциальности информации, т.е. предотвращения несанкционированного считывания информации,

– обеспечения доступности информации, т.е. предотвращение уменьшения пропускной способности информационных каналов.

Геометрия внешнего интерфейса

Поверхность, которая принимает на себя все попытки внешнего вторжения в организм человека – это мембранная поверхность клеток организма.

В работе К. Шмидта-Ниельсена [1], в которую вошли главные результаты его многолетних исследований, проанализированы различные закономерности в ряде организмов от мыши до слона и убедительно показано, что более крупные организмы просто содержат больше клеток, а сами клетки соответствующих органов и тканей примерно одинаковы у разных организмов. Например, диаметр лимфоцита, около 10 мкм, а диаметр обычной клетки печени примерно 20 мкм. Толщина плазматической мембраны составляет около 10 нм.

Известно, что в 1 грамме организма млекопитающего около 1 млрд. клеток. Диаметр одной клетки около 0,01 мм. Тогда, к моменту рождения человека, когда почти все системы организма сформированы, из одной оплодотворенной клетки сформируется мембранная поверхность около $0{,}12*10^4 m^2$. Площадь поверхности всех клеток взрослого человеческого организма составляет около $3*10^4 m^2$ (порядка 10^{14} клеток). Это поле размером 3 га, на котором представлены все внешние вторжения клеток.

На этом поле боя можно выделить передний край: желудочно-кишечный тракт, систему дыхания, кожный покров, органы слуха и зрения (биотопы макроорганизма). Площадь соприкосновения стерильной внутренней среды макроорганизма с внешним микромиром огромна, например, только для тонкой кишки при длине последней 2,8–3,2 м площадь слизистой составляет 180–200м2 .

Этот передний край обороны является интерфейсом организма, через который идет весь поток вторжений и отторжений в процессе взаимодействия с внешним миром.

Под вторжением будем понимать проникновение внутрь организма любых веществ, нарушающих его нормальное функционирование. Отторжение – вывод из организма инородных, вторгшихся веществ и их производных.

Отметим ряд особенностей этого интерфейса.

Частота вторжений и отторжений тем выше, чем меньше площадь вторжения. В этой связи можно высказать гипотезу о существовании ограничений пропускной способности для различных типов внешних биологических информационных каналов.

$$\mapsto \frac{зона_ЖКТ}{\frac{f_1 <}{S_1 >}} \leftrightarrow \frac{зона_К}{\frac{f_2 <}{S_2 >}} \leftrightarrow \frac{зона_Д}{\frac{f_3 <}{S_3 >}} \Leftrightarrow \frac{слух}{\frac{f_4 <}{S_4 >}} \leftrightarrow \frac{зрение}{\frac{f_5}{S_5}} \lrcorner$$

С позиций современной иммунологии каналы звуковой и визуальной информации не рассматриваются как участники формирования иммунного ответа. Для этих каналов пока не известны соответствующие системы комплемента, обеспечивающие вывод вредной информации.

Таким образом, площадь поверхности внешних вторжений:

$$S_i = S_1 + S_2 + S_3,$$

где S_1 – зона ЖКТ – поверхность желудочно-кишечного тракта,

S_2 – зона K – поверхность кожного покрова,

S_3 – зона $Д$ – поверхность системы дыхания.

Площадь S_i составляет около 1% от общей площади мембранной поверхности всех клеток организма.

Рассматриваемую поверхность, имеющая площадь S_i, назовем рабочей Антиген Представляющей Поверхностью (рАПП).

Выделив рАПП, мы вправе утверждать, что не существует других каналов вторжений и отторжений инородных веществ в организм млекопитающего, в каком бы физическом состоянии это вещество не находилось: твердом, жидком или газообразном.

Чтобы исключить потерю существенной информации, проходящей через интерфейс рАПП, оцифровка этой информации должна происходить с частотой не менее чем $2*f3$ (теорема Котельникова).

Важным свойством рАПП, с точки зрения информационной безопасности организма, является непрерывность и конечность этой поверхности.

Поверхность рАПП – геометрическое место точек, для каждой из которых найдется точка этой поверхности, расстояние до которой меньше некоторого наперед заданного числа.

Целостность рАПП является необходимым условием целостности организма. Также как целостность мембранной поверхности отдельной клетки есть условие целостности клетки.

Различие заключается в том, что, если геометрическая модель поверхности клетки может быть аппроксимирована поверхностью шара, то для рАПП, очевидно, этого сделать нельзя.

Для аппроксимации рАПП может быть использована поверхность тора. Эта поверхность имеет следующие ограничения.

Пусть $S_i = l*h$, где l – длина, h – ширина поверхности,

тогда $l > 2*h$,

$\frac{l}{2*\pi} > R_1 > \frac{h}{\pi}$, где R_1 – внешний радиус тора,

$\frac{1}{\pi}*\left(\frac{1}{2} - h\right) > R_2 > 0$, где R_2 – внутренний радиус тора,

$\frac{l - 2\pi R_2}{4} > R_3 > \frac{h - \pi R_2}{2}$, где $R_3 = 2\pi h$ – радиус образующей окружности,

$$4\pi(R_1 + R_2)R_3 < S_i < 4\pi^2 R_2 R_3.$$

Отметим, что рАПП формирует физический и экологический барьер, который препятствует проникновению патологических агентов внутрь организма [2].

Вторжение может быть локализовано в любой точке рАПП. Однако вероятность вторжений различна для различных зон рАПП.

Почти все клетки организма (99%), объекты охраны и обороны иммунной системы, размещены внутри тороидальной рАПП.

Каждая клетка обладает кодом принадлежности данному организму (КПО), который хранится в двух экземплярах как часть кода ДНК. ДНК – это супер-молекула, хранящая закодированную наследственную информацию. Она состоит из двух длинных цепочек химически соединенных попарно. В обычных мерах измерения, длина нити ДНК составляет около 1.82 метра, при толщине 0.0000254 микрон. Это самый длинный код организма.

На поверхности мембраны каждой клетки представлены образы КПО в форме молекул главного комплекса гистосовместимости (МНС – от Major Histocompatibility Complex) [3].

Внутри тороида рАПП выполняется циркуляция крови (кровообращение) и лимфы (хоминг) с опорной частотой пульсаций ≈ 1гц. Циркуляция жидкостей организма гарантирует доставку необходимых средств для решения задач распознавания, переработки и устранения вторжений в любой зоне рАПП.

Предлагаемая геометрическая модель информационного интерфейса организма позвоночных, на наш взгляд, имеет самостоятельную ценность. Тороид рАПП может быть использован для исследований, например, механических вторжений несовместимых с жизнью организма.

С позиций информационной безопасности, клетку организма будем рассматривать как структурно-функциональный элемент, который хранит в двух экземплярах самый длинный код в организме и способен вырабатывать и принимать более короткие коды.

Вторжения

Все возможные вторжения, нарушающие информационную безопасность организма, называют антигенами.

Антигены – (от «против» и греч. génos – рождение, происхождение), высокомолекулярные коллоидные вещества, которые при попадании в организм животных и человека вызывают образование специфических реагирующих с ними антител. Непременным условием антигенности является отличие антигенов от веществ, имеющихся в норме в организме человека.

Определим вторжение как

<вторжение> ::= <антиген>│<пептид>&<эпитоп>.

Знак «::=» означает, что вместо понятия слева от знака может быть подставлено понятие стоящее справа от знака. Знак «│» читается как «или». Знак «&» читается как «и».

Пептид (peptide) – вещество, молекула которого образована из двух или более аминокислот, связанных между собой с помощью аминогруппы (-NH) и карбоксильной группы (-CO). Можно проинтерпретировать как длинный код, упорядоченный набор чисел.

Эпитоп(Epitope) – или антигенная детерминанта (Antigenic determinant, site) – химическая структура на поверхности сложно построенного антигена; в силу особенности своей конфигурации способна взаимодействовать с комплементарной ей структурой в составе антитела (паратопом), определяя тем самым специфичность данной реакции. Можно проинтерпретировать как код, упорядоченный набор чисел.

Процедура распознавания, переработки и устранения вторжений «ответ ИмС»

Алгоритм распознавания, переработки и устранения вторжений выполняется иммунной системой (ИмС). Эту процедуру называют ответом иммунной системы.

Параметры процедуры

Для выполнения процедуры необходимо определить ее переменные, которые назовем адептами ИмС (хранителями тайн) и определим так:

<адепты ИмС> ::=<антитела>│<лимфоциты>│<цитокины>│<фагоциты>│<система комплемента>

<антител > ::= <иммуноглобулин> & <паратоп>

Антитела (antibodies) – белки, образующиеся в организме при попадании в него некоторых чужеродных веществ – антигенов – и обладающие способностью избирательно соединяться с теми же антигенами или (в меньшей степени) со сходными с ними по строению веществами, вызывая тем самым иммунный ответ организма. Длинный код, упорядоченный набор чисел.

Паратоп (paratope) – антигенсвязывающий центр антитела; в силу особенности своей конфигурации способен взаимодействовать с комплементарной ему структурой в составе антигена (эпитопом), определяя тем самым специфичность данной реакции. Можно проинтерпретировать как код, упорядоченный набор чисел.

< иммуноглобулин >::= < IgA > │< IgD >│ < IgE > │ < IgG > │ < IgM >

Иммуноглобулинами называются белки, которые синтезируются под влиянием антигена и специфически с ним реагируют. Иммуноглобулины состоят из полипептидных цепей. Можно проинтерпретировать как длинный код, упорядоченный набор чисел.

< лимфоциты> ::= < Т-лимфоциты > │< В-лимфоциты > │ < NK-клетки >

Лимфоциты – это вид белых кровяных телец (клеток). Различают малые, средние и большие лимфоциты. Малые лимфоциты имеют диаметр менее 8 мкм. Средние лимфоциты имеют сходную с

малыми структуру, размеры их 8–12 мкм. Большие лимфоциты имеют диаметр 12–14 мкм. Лимфоциты составляют основную массу клеточных элементов лимфоидной ткани, 95% клеток лимфы и 30% общего числа лейкоцитов крови.

<Т-лимфоциты>::= <Тn> │ <Т-хелперы> │ <Т-киллеры>│ <Т-памяти>│ <Т-супрессоры>

<Тn> ::= <Т-наивный>

Т-лимфоциты – это средние лимфоциты. Незрелые лимфоциты покидают костный мозг и попадают в кровяное русло. Некоторые из них направляются к тимусу (вилочковой железе), расположенному у основания шеи, где происходит их созревание. Прошедшие через тимус лимфоциты известны как Т-лимфоциты, или Т-клетки (Т от «тимус»). Зрелые Т-лимфоциты представлены в организме различными типами: Т-хелперы, Т-киллеры, Т-памяти, Т-супрессоры. Роль этих клеток поясним при описании алгоритма ответа иммунной системы.

<В-лимфоциты>::= <Вn> │<В-памяти> │ <плазматические клетки>

<Вn> ::= <В-наивный>

В-лимфоциты – это малые и средние лимфоциты. В экспериментах на цыплятах было показано, что часть незрелых лимфоцитов закрепляется и созревает в сумке Фабрициуса – лимфоидном органе около клоаки. Такие лимфоциты известны как В-лимфоциты, или В-клетки (В от bursa – сумка). У человека и других млекопитающих В-клетки созревают в лимфатических узлах и лимфоидной ткани всего организма. Зрелые В-лимфоциты представлены в организме различными типами: В-наивные, В-памяти и плазматические клетки. Роль этих клеток выяснится при описании алгоритма ответа иммунной системы.

Антигенраспознающий рецептор (порт для приема/передачи информации) и функциональные потенции приобретаются лимфоцитами в процессе их развития. При этом срабатывают механизмы, обеспечивающие невозможность формирования на клетке более, чем одного типа рецепторов. В результате каждый созревающий лимфоцит имеет рецепторы, уникальные по специфичности [7,8].

NK-клетки – большие лимфоциты, известные как естественные киллеры.

<цитокины> ::= <интерлейкины>│<интерфероны>│<факторы некроза опухолей>│
<колониестимулирующие факторы>

<интерлейкины>::= <IL-2>│<IL-3>│<IL-4>│<IL-12>│…

<интерфероны>::= <INF-гамма>│…

<факторы некроза опухолей >::=<FNO-α>│<FNO-β>│…

<колониестимулирующие факторы>::=<ГМ-КСФ>│…

Цитокины – это небольшие белки (мол. масса от 8 до 80 КДа), действующие аутокринно (т.е. на клетку, которая их продуцирует) или паракринно (на клетки, расположенные вблизи). Образование и высвобождение этих высокоактивных молекул происходит кратковременно и жестко регулируется. Все клетки ИмС производят цитокины или, по крайней мере, готовы принять сообщение-цитокин через свой порт (рецептор) на мембранной поверхности. Вся совокупность цитокинов определяет трафик обмена информацией внутри организма. Код, упорядоченный набор чисел.

<фагоциты>::= <макрофаги>│<дендритные клетки>│<тучные клетки>│…

Макрофаги – это вид белых кровяных телец лейкоцитов, известных как фагоциты, получившие свое название от греческого phago – «есть» и cyt – «клетка». Они постоянно стремятся «съесть», уничтожить чужеродных «захватчиков», таких, как микроорганизмы, пылинки в легких, патогенные грибки, загрязняющие вещества из дыма и многое другое, что они могут распознать как нагрузку, нежелательную для здоровья организма.

Дендритные клетки (DENDRITIC CELLS) – тип клеток иммунной системы, имеющих длинные, похожие на щупальца, ответвления, которыми они захватывают чужеродные объекты.

Тучные клетки — одна из основных клеточных форм соединительной ткани.

<система комплемента>::= < комплементные белки>│<МАК>

<комплементные белки> ::= <С1>│. . . │<С9>│<фактор В>│ . . .

<МАК > ::= <мембранный атакующий комплекс>

Система комплемента – это совокупность более 25 белков сыворотки крови, циркулирующих в неактивном состоянии. При попадании в ткани (кровь) активаторов (иммунных комплексов <антиген+антитело>) происходит активация системы – каскадное взаимодействие белков системы комплемента с образованием повреждений в мембране клеток-мишеней. Последовательная активация всех компонентов системы комплемента имеет ряд последствий. Во-первых, происходит каскадное усиление реакции, почти каждый последующий этап реакции активации комплемента является ферментативным, при котором продуктов реакции образуется несравнимо больше, чем исходных реагирующих веществ. Во-вторых, на поверхности бактерии фиксируются компоненты комплемента, резко усиливающие фагоцитоз этих клеток, то есть сродство их к фагоцитирующим клеткам организма. В-третьих, при ферментативном расщеплении белков системы комплемента образуются фрагменты, обладающие мощной воспалительной активностью. И, наконец, при

включении в комплекс антиген-антитело последнего компонента комплемента этот комплекс приобретает способность «продырявливать» клеточную мембрану и тем самым убивать чужеродные клетки.

В составе параметров процедуры «ответ ИмС» выделим те из них, которые непосредственно связывают и устраняют вторжения. Назовем эти параметры эффекторами ИмС. К этим параметрам относятся:

1. <фагоциты> – клетки, которые при встрече с антигеном захватывают его без учета специфичности и пытаются переработать внутри клетки,
2. <система комплемента> – набор белков, которые при встрече с комплексом <антиген+антитело> активируются без учета специфики антигена и разрушают данный комплекс, либо клетку, если данный комплекс закреплен на ее поверхности.
3. <антитело> – белок, который при встрече с соответствующим антигеном взаимодействует с ним, образуя иммунный комплекс <антиген+антитело>,
4. <Т-киллеры> – клетки, которые при встрече с клетками, на мембране которых размещен соответствующий антиген и код несоответсвия клетки данному организму (молекула МНС I), атакуют клетку-мишень, вводя внутрь клетки лизирующее (растворяющее) вещество.

Одной из ключевых функций иммунной системы является управление синтезом эффекторов ИмС и регулирование их численности.

Условие запуска процедуры «ответ ИмС»

Для запуска иммунного ответа на новое (ранее не встречавшееся) вторжение необходима локализация следующих условий [4,5,6,7]:

– меется поверхность (мембрана) антигенпрезентирующей клетки – АПК (макрофага или дендритной клетки или В-лимфоцита),
– на поверхности АПК зафиксирован пептид с антигенной детерминантой (эпитопом),
– на поверхности АПК зафиксирована молекула МНС II – идентификатор организма-хозяина,
– с этой поверхности стартует (экспрессирует) цитокин-сообщение (IL-2), которое, в частности, подтверждает события 1,2,3.

Коротко условие запуска процедуры запишем так:

$$\text{<АПК>\&< молекула МНС II >\&< антиген>} \xrightarrow{<IL-2>}$$

<АПК>::=<антингенпрезентирующая клетка>│<макрофаг>│<В-лимфоцит>│<дендритная клетка>

Данное событие связано с передачей информации о локализации вторжения и о специфике антигена. Эта информация передается ближайшему **подходящему** «наивному» Т-лимфоциту. Получивший информацию Tn активируется. Начинается процесс деления (пролиферации) активированной Т-клетки. При этом может быть произведено от 500 до 1000 клеток. Вся вновь возникшая популяция поступает в поток циркуляции жидкостей организма, чтобы добраться до тимуса и там завершить свое развитие.

$$\text{< АПК >\&< молекула МНС II >\&< антиген >} \xrightarrow{\text{IL2}} < Tn_i^a >, \qquad (1)$$

где $< Tn_i^a >$ – активная «наивная» Т-клетка, обладающая информацией об антигене,

знак «$\xrightarrow{<условие>}$» означает необходимое преобразование понятия слева от стрелки в понятие справа от стрелки при исполнении заданного условия.

Событие (1) указывает на то, что вторжение обнаружено! Информация о локализации вторжения и его коде (или часть этой информации) записана в клетке $< Tn_i^a >$.

Событие (1) также говорит о том, что в окружении АПК нет эффекторов ИмС.

В результате события (1) формируется клон клеток $< Tn_i^a >$ [15]. Обозначим клон клеток как $<< Tn_i^a >>$.

Синтез эффекторов иммунной системы

Созревание клеток $<< Tn_i^a >>$ связано с развитием конкретных рецепторов (портов) и конкретных функциональных потенций (дифференцировка) клеток.

Из конкретной $< Tn_i^a >$ может созреть либо <Т-киллер>, либо <Т-хелпер>, либо <Т-супрессор>, либо остановиться в развитии в виде <Т-памяти>.

$$\text{< Т-хелпер > ::= } < Tn_i^a > \text{\&<рецептор CD4>}$$

$$\text{< Т-памяти > ::= } < Tn_i^a > \text{\&<рецептор памяти>}$$

$$\text{< Т-супрессор > ::= } < Tn_i^a > \text{\&<рецептор торможения>}$$

< Т-киллер > ::= $< Tn_i^a >$ &<рецептор CD8> | <ЦТЛ>

< ЦТЛ > ::= < цитотоксический Т-лимфоцит>.

Количественное распределение производных типов клеток от клона $<< Tn_i^a >>$ – вопрос требующий специального рассмотрения.

Если в результате созревания клеток из клона $<< Tn_i^a >>$ популяция Т-киллеров не пуста, то одна из промежуточных задач ответа ИмС решена – синтезирован (ы) специализированный эффектор для переработки вторжения (1) – $< ЦТЛ_i^a >$.

Синтез других эффекторов ИмС связан с дальнейшим развитием Т-хелперов [6].

< Т-хелпер > $\xrightarrow{<IL-12>\&<INF-\gamma>}$ < Th клеточной активности> | $< Th1_i^a >$

< Т-хелпер > $\xrightarrow{<IL-4>}$ < Th гуморальной активности> | $< Th2_i^a >$ (от лат. *humor* – жидкость)

Клетки $< Th1_i^a >$ и $< Th2_i^a >$ являются генераторами своего (отличающегося) набора цитокинов.

Если популяция $< Th1_i^a >$ от клона $<< Tn_i^a >>$ не пуста, то стимулируется активность фагоцитов и ЦТЛ, подтверждая информацию о событии (1). Под активностью соответствующих клеток следует понимать увеличение их числа в области вторжения.

$< Th1_i^a > \xrightarrow{<C_k>}$ <активность фагоцитов и ЦТЛ>

$< C_k >$ ::=<цитокины_клеточной_активностью> | <IL2> | <IFN-γ> | <Il3> | <FNO-α> | <FNO-β> | <ГМ-КСФ>.

Если популяция $< Th2_i^a >$ от клона $<< Tn_i^a >>$ не пуста, то стимулируется активность В-лимфоцитов и передается информация о событии (1).

$< Th2_i^a > \xrightarrow{<C_g>}$ <активность В-лимфоцитов>

$< C_g >$ ::=<цитокины_гуморальной_активностью> | <IL4> | <IL5> | <IL3> | <IL6> | <IL9> | <IL13> | <ГМ-КСФ>.

Активность В-лимфоцитов приводит к синтезу наиболее эффективных средств борьбы с вторжением (1) – специализированных антител [13,14]. Информация от $< Th2_i^a >$ передается ближайшему «наивному» В-лимфоциту. Образуется клон $<< Bn_i^a >>$, из которого созревают либо плазматические клетки, либо (и) клетки В-памяти.

< плазматическая клетка >::= $< Bn_i^a >$ &< рецептор антитела >

< В-памяти > ::= $< Bn_i^a >$ &< рецептор памяти >

Плазматическая клетка обладает способностью к синтезу и выделению в жидкости организма антител, необходимых для связывания антигена, обнаруженного при возникновении события (1).

$< Bn_i^a >$ &< рецептор антитела > $\xrightarrow{?} < антитело_i >$

Знак «?» говорит о том, что автору неизвестны условия освобождения белков $< антитело_i >$.

Из всего выше сказанного следует, что событие (1) порождает лавинообразный процесс синтеза эффекторов иммунной системы. Любой из синтезированных эффекторов ИмС способен ликвидировать единичный факт вторжения. Поэтому процедура «ответ ИмС» имеет набор методов и средств сдерживания процесса синтеза эффекторов и уменьшения их активности. Основным инструментом устранения избытка эффекторов ИмС является процедура апоптоза. Термин «апоптоз» (с греч. – опадание листьев) введен в научный обиход в 1972 году для обозначения формы гибели клеток. Апоптоз – это активная форма гибели клетки, являющаяся результатом реализации ее генетической программы или ответом на внешние сигналы и требующая затрат энергии и синтеза макромолекул de novo, проявляющаяся в уменьшении ее размера, конденсации и фрагментации хроматина, уплотнении наружной и цитоплазматических мембран без выхода содержимого клетки в окружающую среду.

Переработка вторжений

Переработку вторжений выполняют синтезированные иммунной системой эффекторы, специализированные белки и клетки, получившие информацию о вторжении. Ликвидация одного и того же единичного вторжения может быть выполнена с помощью различных эффекторов ИмС [5,9,10,11,12].

1. Поглощение антигена фагоцитом.

$$< антиген_i > \& < фагоцит^a > \xrightarrow{?} < фагоцит^a >$$

Если антиген успешно перерабатывается внутри клетки фагоцита, то процесс ликвидации единичного вторжения завершен, в противном случае возникает событие (1).

2. Разрушение зараженной клетки цитотоксическим лимфоцитом.

$$< клетка - мишень > \& < молекула_MHC_I > \& < антиген_i > \Leftrightarrow < ЦТЛ_i^a >$$

Объектом атаки специализированного Т-киллера $< ЦТЛ_i^a >$ являются клетки (клетки-мишени), на поверхности которых размещены как $< антиген_i >$, так и молекула МНС I – фрагмент КПО, признак «не свой». Атака $< ЦТЛ_i^a >$ завершается введением внутрь клетки-мишени лизирующего (растворяющего) вещества. После этого $< ЦТЛ_i^a >$ переходит к поиску очередной жертвы.

3. Формирование иммунного комплекса.

$$< антиген_i > \xrightarrow{< антитело_i >} < антиген_i + антитело_i >$$

Встреча антигена с соответствующим антителом с необходимостью приводит к образованию иммунного комплекса $< антиген_i + антитело_i >$, который сам по себе, в большинстве случаев, уже не опасен для организма. Зафиксированный на поверхности клетки-мишени иммунный комплекс $< антиген_i + антитело_i >$ с необходимостью приводит к активированию системы комплемента и разрушению мембраны зараженной клетки.

$$< клетка - мишень > \& < антиген_i + антитело_i > \& < система_комплемент\ a >$$

Все результаты исполнения процедуры «ответ ИмС» (метаболиты), отторжения, образованные в результате действий эффекторов ИмС, локализуются на поверхности рАПП и покидают организм в твердом, жидком или газообразном состоянии.

Выводы

1. В сложной биологической системе каждая клетка – структурно-функциональный элемент (СФЭ) обладает признаком принадлежности данной системе. Этот признак доступен для контроля со стороны системы информационной безопасности.

2. Каждый СФЭ может быть восстановлен двумя способами. Путем синтеза из одной (стволовой) клетки. Аналог восстановления программы из исходных текстов. Либо путем самокопирования (деление клеток).

3. Каждый СФЭ лоялен к системе информационной безопасности. Это выражается в инициативе выдачи сообщения о нарушении структуры или исполняемых функций. Кроме того, СФЭ обладает способностью запускать внутреннюю процедуру апоптоза.

4. В сложной биологической системе реализуется более одного способа удаления вторжений.

5. Возможно, для каждого вторжения существует отторжение.

СПИСОК ЛИТЕРАТУРЫ

1. Шмидт-Ниельсен К. Размеры животных: почему они так важны?, М.,Мир,1987,–259с.
2. Хэм А., Кормак Д. Гистология, М., «Мир», т. 4, 344 с.
3. Marsh S.G.,Albert E.D.,Bodmer W.F.,Bontrop R.E., Dupont B., Erlich H.A., Geraghty D.E., Hansen J.A., Mach B.,Mayr W.R.,Parham P., Petersdorf E.W.,Sasazuki T.,Schreuder G.M., Strominger J.L., Svejgaard A.,Terasaki P.I., 2002. Nomenclature for factors of the HLA system, 2002. Tissue Antigens 60,407–464.
4. Петров Р.В. Формы взаимодействия клеток лимфоидных тканей: трехклеточная система иммуногенеза. Успехи совр. биол. 194: 1208–1210. 1970.
5. Germain R.N., Castellino F., Han R. et al. Processing and presentation of endocytically acquired protein antigens be MHC class II and class I molecules. Immunol.Rev.151: 5–30.1996.
6. Madden D.R. The three-dimensional structure of peptide-MHC complexes. Ann. Rev. Immunol.13: 587–622.1995.
7. Nicholson L.B., Kichroo V.K. T cell recognition of self and altered self antigens Crit. Rev. Immunol. 17: 449–462.1997.
8. Cantrell D. T cell antigen receptor signal transduction pathways. Ann. Rev. Immunol.12: 259–274.1996.
9. Хаитов Р.М., Алексеев Л.П. Роль HLA-антигенов в клеточном взаимодействии. Иммунология. 5: 11–15. 1998.
10. Janeway C.A. The T cell receptor as a multicomponent signalling machine: CD4/CD8 coreceptors and CD45 in T cell activation. Ann.Rev. Immunol.10:645-674.1992.
11. Moller G. The B-cell antigen receptor complex. Immunol. Rev. 132:1–206. 1993.
12. Zinkernage R.M., Doherty P.C. The discovery of MHC restriction. Immunol. Today.18: 14–17.1997.
13. Capra J.D. Germinal centers . Immunologist. 4: 84–86.1996.
14. Noelle R. B-cell differentiation and antibody production. Immuniologist. 3:219–220.1995.
15. Sprent J. T and B memory cells. Cell.– 1994.– Vol. 76.– P. 315–322.
16. Тараканов А., Дасгупта Д. Архитектура иммуночипа и ее эмуляция. Конференция НАСА/МО по эволюционируемой аппаратуре, ЕН-2002, с. 261-265. Александрия, Вирджиния, 15–18 июля 2002.
17. Тараканов А.О. Формальные иммунные сети: математическая теория и технология искусственного интеллекта. Теоретические основы и прикладные задачи интеллектуальных информационных технологий (ред. Юсупов Р.М.). СПб, СПИИРАН, 1998, 65–70.
18. Tarakanov A.O., Skormin V.A., Sokolova S.P. Immunocomputing: Principles and Applications. Springer, New York, 2003.
19. Блюм В.С., Заболотский В.П. Иммунная система и иммунокомпьютинг. Математическая морфология. Электронный математический и медико-биологический журнал (том 6 выпуск 4 2007).

УДК 004.056

ПРИНЦИПЫ СЕМИОТИЧЕСКОГО МОДЕЛИРОВАНИЯ КОНФЛИКТУЮЩИХ СИСТЕМ В ПРИЛОЖЕНИИ К ЗАДАЧЕ ВНЕШНЕГО ПРОЕКТИРОВАНИЯ ПРОАКТИВНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Горбачев Игорь Евгеньевич, Якунин Владимир Иванович,
Военно-космическая академия им. А.Ф. Можайского,
Россия, Санкт-Петербург, ул. Ждановская, д. 13,
e-mail: gie1976@mail.ru

Аннотация: В статье представлен концептуальный подход к проектированию проактивных систем информационной безопасности. Раскрываются существенные ограничения применяемого научно-методического аппарата моделирования сложных объектов. Представлены недостатки теории автоматов, лежащей в основе создания реактивных средств защиты информации. Основная идея статьи заключается в необходимости применения методов прикладной семиотики, позволяющей устранить существующие концептуальные ограничения при проектировании систем информационной безопасности.

Ключевые слова: *проектирование; конфликтующие системы; информационная безопасность; проактивная технология; семиотическое моделирование; ситуационное управление.*

PRINCIPLES OF CONFLICT OF MODELING SEMIOTIC AS APPLIED TO EXTERNAL DESIGN PROACTIVE INFORMATION SECURITY SYSTEMS

Igor Gorbachev, Vladimir Yakunin,
Federal State Establishment «Mozhaisky Military Aerospace Academy»,
Russia, St. Petersburg, Zhdanovskaya street 13,
e-mail: gie1976@mail.ru

Abstract: The paper presents a conceptual approach to the design of proactive information security systems. Disclosed are significant limitations to apply scientific-methodical device modeling complex objects. Presents disadvantages automata theory underlying the creation of reactive protection information. The main idea of the article is the need to use methods of applied semiotics, which allows to remove the existing restrictions on the conceptual design of information security systems.

Keywords: *design; conflicting systems; information security; proactive technology; semiotic modeling; contingency management.*

Введение. Особенностью взаимодействия конфликтующих целеустремленных систем (КЦС) в информационном конфликте являются одинаковые условия функционирования их средств информационного нападения и защиты. Под условиями функционирования следует понимать некоторую среду – «площадку», на которой происходит конфликт. В киберпространстве этой средой является критическая информационная инфраструктура (КИИ), характеристики которой (вектор $B'_{\langle l' \rangle}$) оказывают влияние на параметры и эксплуатационно-технические характеристики КЦС (вектор $A'_{\langle k' \rangle}(B'_{\langle l' \rangle})$), а также на характеристики (вектор $A''_{\langle k'' \rangle}(B'_{\langle l' \rangle})$) технологии (процесса организации) компьютерных воздействий (КВ), проводимых КЦС, и через них обусловливающие возможные результаты $U_{\langle 3 \rangle} = U_{\langle 3 \rangle}(A'_{\langle k' \rangle}, A''_{\langle k'' \rangle}; B'_{\langle l' \rangle})$ этих воздействий. Вектор $U_{\langle 3 \rangle}$ характеризует потенциал компьютерного воздействия нарушителя – участника информационного конфликта в киберпространстве [1].

Применение средств КВ происходит в условиях активного противодействия системы защиты атакуемой стороны (характеристики которой обозначим через вектор $B''_{\langle l'' \rangle}$), влияющей на ситуацию и тем самым обуславливающей для нарушителя требуемые $U^{\partial}_{\langle 3 \rangle}(B''_{\langle l'' \rangle})$ результаты КВ, т.е. $U_{\langle 3 \rangle} \in \{U^{\partial}_{\langle 3 \rangle}\}$ [7]. Соотношение $U_{\langle 3 \rangle} \in \{U^{\partial}_{\langle 3 \rangle}\}$ представляет собой формальное выражение цели КВ, в то время как содержательно цель определяется следующим образом: нарушение работоспособности объекта КИИ путем создания доминирующих в киберпространстве конфликтующих целенаправленных процессов (КЦП) – процессов нарушения информационной безопасности (ИБ). Представленные выше векторы образуют так называемый операционный комплекс моделирования процессов нарушения ИБ, структура которого представлена в [2].

Следует отметить, что взаимодействие КЦС в КИИ представлено в виде КЦП, характеристики которых являются характеристиками $A''_{\langle k'' \rangle}$ технологии КВ, проводимых КЦС. Таким образом, можно

говорить о возникновении двуединой задачи, заключающейся, с одной стороны, в моделировании объектов КИИ как среды взаимодействия КЦС – вектор $B'_{\langle l' \rangle}$, с другой стороны, в моделировании киберпротивника $U_{\langle 3 \rangle}$, представленного в КИИ в виде КЦП (вектор $A''_{\langle k'' \rangle}$). Этапы моделирования киберпротивника подробно представлены в [3].

Анализ специфики построения и особенностей функционирования КИИ в аспекте возможности моделирования действий нарушителя и проектирования проактивных систем и средств ИБ позволяет отнести объекты КИИ к сложным системам. Приведем характеристики $B'_{\langle l' \rangle}$ (но не формальные признаки) этих объектов, характеризующих их как сложную систему.

1. Уникальность объекта. Объекты КИИ обладают уникальной структурой и индивидуальными особенностями своего функционирования. Как следствие, низкая возможность успешного применения нарушителем какой-либо типовой стандартной процедуры КВ. Это обстоятельство удорожает процедуру построения системы ИВ.

2. Сложность в четкой формализации цели функционирования объекта и критериев оптимального управления. Для большинства объектов КИИ практически невозможно формализовать цель их функционирования. В результате, нельзя математически четко задать критерии работоспособности объекта и критерии оптимального управления им. Как следствие, низкая возможность математического описания цели $U_{\langle 3 \rangle} \in \{U^{\partial}_{\langle 3 \rangle}\}$ воздействия в аспекте возможности нарушения работоспособности объекта КИИ, то есть невозможность математического формулирования критерия пригодности компьютерной атаки по ее результатам (критерия, оценивающего качество результатов КВ).

3. Нестационарность объекта. Нестационарность объекта КИИ проявляется в эволюции числа и значений характеристик объекта во времени, когда с течением времени изменяется его структура и функционирование. Проявляется эта черта в различной реакции объекта на одну и ту же ситуацию или воздействие в различные моменты времени. Поэтому при синтезе модели объекта КИИ необходимо вводить ее динамичную коррекцию. Это создает серьезные трудности при синтезе модели воздействия на объект. Как следствие, проектируемые системы моделирования КВ должны быть адаптивными, готовыми к изменению своего функционирования.

4. Организационная система. Обязательными элементами структуры объектов КИИ являются люди. В отличие от других элементов КИИ люди обладают свободой действий в рамках функционирования объекта и управления им с учетом своих личных интересов и целей. Вследствие этого их внешнее управление нарушает «нормальное» функционирование объекта, т.е. изменяет его самостоятельное поведение и делает зависимым от субъекта.

В результате, на этапе внешнего проектирования облика проактивной системы ИБ возникают следующие актуальные задачи, предшествующие собственно задаче априорного оценивания эффективности КВ нарушителя:

1. Задача математического обоснования показателя V целевого эффекта – результативности КВ (т.е. результата, ради которого проводится КВ). Показатель V является одной из компонент комплексного показателя потенциала нарушителя $U_{\langle 3 \rangle} = \langle V, R, T \rangle$, где R – показатель ресурсоемкости КВ, T – показатель оперативности КВ.

2. Задача математического обоснования критерия оценивания качества результатов КВ: $U_{\langle 3 \rangle} \in \{U^{\partial}_{\langle 3 \rangle}\}$.

Для разрешения данных задач необходимо, (но не достаточно) создание математической модели защищаемого объекта КИИ. Такая постановка задачи позволяет сформулировать следующее утверждение: для моделирования формальных методов воздействия на сложную систему необходимо создание ее адекватной математической модели.

В области ИБ задача построения адекватной математической модели сложного объекта защиты в настоящее время полностью не решена. Более того, нет единой методологии разработки таких моделей в данной предметной области. Поясним данную проблемную ситуацию.

Традиционная теория автоматического управления техническими объектами исходит из положения, что любой объект управления (далее объект воздействия) может быть формально описан в виде достаточно простой математической модели. В качестве такой модели используются различного рода дифференциальные уравнения. В более сложных случаях модель может представлять собой систему интегро-дифференциальных уравнений или смешанную систему, в которую наряду с дифференциальными уравнениями входят алгебраические и другие уравнения, связывающие между собой параметры, описывающие структуру или процесс функционирования объекта.

Формализация такого типа считается необходимым и достаточным условием поиска оптимального способа воздействия на объект, а возможность такой формализации всегда постулируется. Другими словами, задача воздействия априори считается формализованной, то есть в зависимости от вида уравнений, описывающих поведение объекта и системы воздействий на него, а также в зависимости от того критерия воздействия, который был задан, выбирается пригодный метод поиска оптимального воздействия. Данные методы поиска широко известны в традиционной теории управления (методы линейного программирования, методы динамического программирования и другие), а класс исследуемых в данной теории объектов принято называть простым.

В соответствии с [5] под простым объектом понимается объект, для управления которым необходима и достаточна формальная теория объекта. Некоторые простые объекты управления могут не иметь математического описания, однако если простыми объектами можно управлять без их математической модели, то сложными уже нельзя.

К простым объектам следует отнести и так называемый класс сложных формализуемых систем, на которых остановимся подробнее. В разное время предлагались различные математические модели таких сложных систем: диагностируемая система Дмитриева А.К., Юсупова Р.М., агрегативная система Бусленко Н.П., непрерывно-дискретная система Глушкова В.М., гибридная система А. Пнуэли и многие другие. Каждый из авторов предлагает свою модель и новый формальный подход к описанию, как они предполагают, нового класса сложных систем. Результат анализа показывает, что в действительности в этих трудах исследуются один и тот же класс динамических систем с переменной структурой, характерной для производственных процессов, для исследования которых не всегда пригодны классические методы прикладной математики – в этом и заключается «сложность» данных систем. Для моделирования их поведения и структуры используются формальные методы теории массового обслуживания, теории игр и статистических решений, теории автоматов, теории статистического моделирования и др., а сама автоматизированная система управления рассматривается как единая сложная система совместно с управляющими подсистемами. Делается попытка унификации структуры моделей на базе так называемых агрегативных систем, позволяющих с единой точки зрения описывать процессы различной природы. Такие сложные динамические системы часто называют гибридными системами (что абсолютно правильно), поведение которых обусловлено совместным функционированием непрерывных и дискретных объектов; мгновенными качественными изменениями в непрерывном объекте; изменением состава системы.

Следует заметить, что в технической литературе часто используются термины «смешанная система», «агрегативная система», «непрерывно-дискретная система», «система с переменной структурой», «событийно-управляемая система», семантика которых не всегда понятна. Объективное исследование этого противоречия представлено в работе [6], результатами этого анализа является доказательство приводимости различных математических моделей сложных систем друг к другу. На основании чего может быть сделан вывод о том, что представленные выше термины являются синонимами и описывают один класс простых объектов.

Традиционная схема управления простыми объектами представлена на рисунке 1.

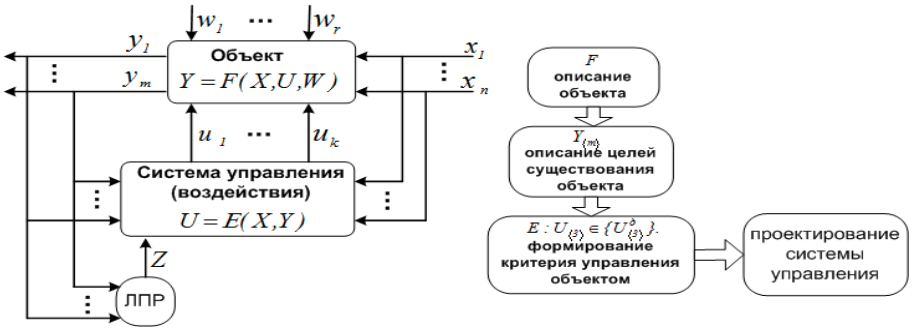


Рис. 1. Традиционная схема управления простыми объектами

В соответствии с рисунком 1 для моделирования системы воздействия на объект требуется определить: множество предпочтительных векторов $Y_{\langle m \rangle}$ и отображение F. Отображение F описывает специфику построения и особенности функционирования объекта воздействия, а знание предпочтительных значений $Y_{\langle m \rangle}$ говорит о понимании цели его функционирования. Эти сведения позволяют сформулировать критерий E оптимального воздействия на объект, $E : U_{\langle 3 \rangle} \in \{U^{\partial}_{\langle 3 \rangle}\}$. Критерий E может быть различным, но именно наличие критерия воздействия позволяет ставить и решать традиционную задачу проектирования системы управления простым объектом (рисунок 1).

Традиционная схема проектирования системы воздействия на простые объекты имеет ряд ограничений. Как правило, специалисты прилагали усилия лишь к поиску процедуры управления

объектом, когда F, $Y_{\langle m \rangle}$, E были уже описаны в точных терминах. То есть простой объект воздействия, как правило, заменялся некоторой синтаксической формальной моделью – некоторым уравнением. Далее независимо от семантики решаемой задачи, применялись различные методы нахождения оптимального управления. По сути, простой объект синтаксически формализуем и моделируется конечным автоматом с дискретным временем либо, в случае гибридных систем, гибридным автоматом с различными моделями непрерывного времени, а сама конструкция автомата предопределяется двумя свойствами объекта управления – его полной управляемостью и идентифицируемостью.

Для управления сложными объектами формальная синтаксическая модель объекта не применима. Действительно, как объект КИИ, так и киберпротивник – это неидентифицируемые и трудно управляемые объекты воздействия. Отсюда возникает проблема идентификации этих сложных информационных объектов и проблема выявления критериев оптимального управления ими. Как следствие, все трудности воздействия определяются сложностью объекта, поэтому следует начинать именно с моделирования объекта, а не с алгоритма управления им.

Рассмотрим в самом общем виде постановку задачи воздействия на сложный информационный объект. Под текущей ситуацией на объекте воздействия будем называть совокупность всех сведений о структуре объекта воздействия и его функционировании в данный момент времени. Под полной ситуацией будем называть совокупность, состоящую из текущей ситуации, знаний о состоянии системы воздействия в данный момент и знаний о технологии воздействия. Обозначим полные ситуации через S_i, а текущие ситуации через Q_j. Пусть в распоряжении системы воздействия имеется n различных способов воздействия на объект атаки – одношаговых решений U_k. Элементарный акт воздействия можно представить в следующем виде: $S_i; Q_j \underset{U_k}{\Rightarrow} Q_l$. Физический смысл этого соотношения заключается в следующем. Если на объекте воздействия сложилась ситуация Q_j и состояние системы воздействия, определяемое S_i, допускают использование воздействия U_k, то оно применяется. Текущая ситуация Q_j превращается в новую ситуацию Q_l. Подобные правила преобразования будем называть логическими правилами (ЛП), а их список задает возможности системы воздействия влиять на процессы, протекающие в объекте. Данная постановка задачи воздействия на сложный объект основана на введении понятия ситуации, классификации ситуации и их преобразовании. Методы воздействия в рамках данной постановки задачи будем называть методами ситуационного воздействия по аналогии с методом ситуационного управления Поспелова Д.А. [8].

Под формальной моделью будем понимать четверку $\mathrm{M} = T, P, A, \Pi$, где T – множество базовых элементов, P – синтаксические правила, A – система аксиом, Π – семантические правила. В синтаксических системах, описывающих простые объекты, T, P, A, Π остаются неизменными. Это означает, что если бы формальные системы использовались для создания ситуационных моделей воздействий на сложные объекты, то язык описания ситуаций (он определяется T и P), исходные знания об объекте воздействия и законах воздействия (они определяются заданием множества аксиом A) и ЛП (они совпадают с семантическими правилами Π) оставались бы неизменными.

Как видно, это противоречит характерным чертам сложных объектов, так как система воздействия на них, базирующаяся на формальной синтаксической модели и моделируемая автоматом, априорно должна иметь всю информацию, которая остается для нее неизменной в течение всего периода воздействия. Теорию автоматов, лежащую в основе большинства современных кибернетических устройств, еще называют стимульно-реактивной теорией [9] автоматов в силу того огромного значения, которое играет для этой теории психологическая схема «стимул-реакция». Однако, следует признать, что моделирующие возможности современных автоматов все еще невысоки. Так, не вполне удачны предпринимаемые в кибернетике попытки смоделировать с помощью стимульно-реактивных устройств процесс принятия решения человеком. Характерны в этом отношении неудачи так называемого эвристического программирования, используемого в технологии проактивной защиты. В области ИБ примерами стимульно-реактивных устройств являются антивирусные средства, системы обнаружения атак и другие средства, в основе функционирования которых заложена реактивная (сигнатурная) технология, недостаток которой очевиден.

Уникальность сложного объекта требует для описания его структуры, функционирования и особенностей поведения специальных семантических и прагматических формальных моделей. Это требует специальных языковых средств для описания таких моделей. К сожалению, классическая математика не позволяет сделать это. Выход из создавшейся проблемной ситуации видится в применении методов ситуационного управления и семиотического моделирования, разработанных в рамках прикладной семиотики.

В прикладной семиотике одно из центральных мест занимает понятие семиотического моделирования. Суть семиотического моделирования заключается в следующем. В процессе функционирования системы воздействия на сложные объекты могут корректироваться языки описания ситуаций, изменяться знания об объекте и методах воздействия на него. Это означает, что все элементы, входящие в определение формальной синтаксической модели M, могут изменяться в процессе ее функционирования. С этой целью рассматривается семиотическая модель вида $C = < M, \chi_T, \chi_P, \chi_A, \chi_\Pi >$, предложенная Поспеловым Д.А. Здесь $\chi_T, \chi_P, \chi_A, \chi_\Pi$ соответственно правила изменения T, P, A, Π. Правила χ_T, χ_P меняют синтаксис базовых элементов и их совокупностей, правила χ_A, χ_Π – семантику и прагматику этих совокупностей.

Раскроем физический смысл элементов семиотической модели, точнее. Модель M детерминирована и неизменна. Правила χ_Π дают возможность отказаться от этого, сделать ЛП переменными, например, адаптивными. Примерами таких ЛП могут служить ЛП с вероятностной перенастройкой вида $S_i; Q_j \underset{U_k}{\Rightarrow} (Q_{l1}, q_1; Q_{l2}, q_2; ...; Q_{lr}, q_r)$. В таком ЛП текущая ситуация Q_j при полной ситуации S_i преобразуется не в одну фиксированную текущую ситуацию Q_l, как было ранее, а в r различных текущих ситуаций. Выбор того или иного преобразования осуществляется вероятностным механизмом q_i. В зависимости от удачи или неудачи применения такого ЛП происходит изменение распределения. Такой способ ЛП позволяет подстраивать семантические правила под тот объект, для которого построена система воздействия.

Знания об объекте, его состоянии, а также состоянии системы воздействия можно выразить в виде набора аксиом χ_A. Они служат источником вывода о том воздействии U_k^*, которое необходимо применить в данном случае. В другой момент времени $t+1$ эти знания будут уже другими. Например, было обновлено программное обеспечение на некоторых хостах компьютерной сети, и реализация воздействии $U_k^*(t+1)$ будет неудачным. Поэтому система аксиом должна адекватно меняться с учетом изменений предметной области. Эти изменения можно явно указывать, например, в правых частях ЛП, записывая их в виде $S_i; Q_j \underset{U_k}{\Rightarrow} Q_l; I_i$. Здесь I_i – изменения аксиом, задаваемых правилами χ_A, которые необходимо внести в описание полной ситуации S_i после перехода Q_j в Q_l.

Изменения синтаксических правил могут свидетельствовать, что язык описания ситуаций на объекте, полные знания о нем и процедурах воздействия оказался слишком бедным. Например, в зависимости от текущей ситуации, возникает необходимость использовать разные модели представления объектов КИИ, например, теоретико-множественная модель, модель в виде древовидной (иерархической) структуры, модель в виде семантической сети структуры. Функции такого изменения выполняют правила χ_P. Правила χ_T добавляют в список исходных знаний об объекте новые элементы или исключают из него те, которые оказались ненужными для целей воздействия. Семиотическую модель системы воздействия на сложный объект (или семиотическую модель целеустремленной конфликтующей системы или систему воздействия, базирующейся на семиотической модели) можно представить в виде сети, показанной на рисунке 2.

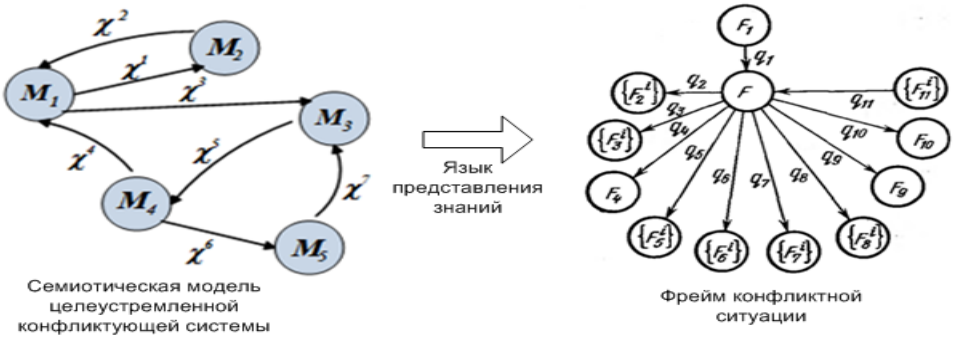


Рис. 2. Пример типовой семиотической модели целеустремленной конфликтующей системы

Каждая вершина сети есть некоторая формальная синтаксическая система M^i, связи между вершинами есть переходы от одной системы M^i к другой под влиянием изменений χ^j. Эти

изменения могут совпадать с χ_T, χ_P, χ_A или $\chi_П$ или быть какой-то их комбинацией. За один такт работы семиотической модели в зависимости от содержимого I_i модель либо останется в том же состоянии (в рамках той же формальной системы), что и ранее, либо перейдет в новое состояние.

В качестве языка для описания текущих и полных ситуаций, характеризующих объект воздействия и систему воздействия, можно использовать язык ситуационного управления, язык RX-кодов, язык исчисления предикатов первого порядка, универсальный семантический код.

Представленные выше логические языки описания конфликтных ситуаций требуется преобразовать в специальные языки представления знаний для организации удобной машинной обработки. В качестве моделей представления знаний предлагается использовать фреймовые модели (рисунок 2).

Каждый фрейм должен представлять готовую структуру, которая при том или ином заполнении слотов значениями превращается в описание конкретной конфликтной ситуации. Фреймы-прототипы должны хранить знания о предметной области, а конкретные фреймы пополнять эти единицы знания реальными данными. Это позволит классифицировать различные конфликтные ситуации, описать способы их обнаружения, и, как следствие, предложить способы устранения конфликтных ситуаций.

Пример. Пусть F – фрейм-прототип, F_1 – фрейм хранения конкретные данных о возникшем конфликте, например, данные о возможном потенциале $U_{\langle 3 \rangle}$ нарушителя [4]. Эти данные используются во фрейме F для понимания целостной картины конфликта и выбора модели, пригодной для исследования нарушителя. Множество $\{F_2^i\}$ – фреймы, которые требуется анализировать при возникновении конфликта, описанного во фрейме F_1. Множество $\{F_3^i\}$ содержит фреймы, в которых содержится информация, характеризующая тот класс конфликтных ситуаций, к которому принадлежит ситуация, составляющая значение слотов в F_1. В качестве примера можно привести детерминированные, стохастические и неопределенные ситуации, возникающие в процессе моделирования нарушителя и его воздействий [3]. Множества $\{F_5^i\}-\{F_8^i\}$ – множества фреймов, в которых содержатся способы устранения конфликта, возникшего, например, при нарушении работы структурных подразделений на объекте защите, при отклонениях показателей штатного функционирования технологического процесса, при анализе журналов аудита ИБ. В фрейме F_9 может формироваться оценка степени конфликтности возникшей ситуации. Фрейм F_{10} фиксирует динамику развития конфликтной ситуации, хранит те мероприятия, которые уже были применены для уменьшении степени конфликтности ситуации. Наконец, множество фреймов $\{F_{11}^i\}$ хранит информацию, необходимую для анализа причин возникновения конфликтной ситуации. Движение по всем связям q_i, показанным на рисунке 2, происходит за счет процедуры, которая хранится во фрейме прототипе F.

Заключение. В основе внешнего проектирования проактивных систем ИБ должна лежать концепция семиотического моделирования и ситуационного управления сложными объектами. За рамки статьи были выведено рассмотрение принципов рефлексивного управления нарушителем ИБ [4], которые должны составлять существо «проактивности» проектируемых современных средств ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Горбачев И.Е. Методологические основы оценивания эффективности действий сторон информационного конфликта в инфотелекоммуникационных системах / И.Е. Горбачев, М.А. Еремеев, Д.В. Андрушкевич // Материалы 23-й науч.-практич. конф. «Методы и технические средства обеспечения безопасности информации». СПб.: Изд-во Политехн. ун-та, 2014. – С. 11–13;
2. Горбачев И.Е. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / И.Е. Горбачев А.П. Глухов // Труды СПИИРАН. – 2015. – № 1(38). – С. 112–133;
3. Горбачев, И.Е. Принципы оценивания потенциала нарушителя и результативности его информационных воздействий в инфотелекоммуникационных системах / И.Е. Горбачев, М.А. Еремеев, Д.В. Андрушкевич // Защита информации. INSIDE. – С-Пб.: ООО «Издательский дом «Афина». – 2014. – № 6(60). – С. 56–64;
4. Горбачев И.Е. Принципы рефлексивного управления нарушителем в инфотелекоммуникационных системах на основе технологии маскирования информационных ресурсов / И.Е. Горбачев, А.Ю. Кудрявцев // Защита информации. INSIDE. – С-Пб.: ООО «Издательский дом «Афина». – 2015. – № 1(61). – С. 2–8;
5. Евменов В.П. Интеллектуальные системы управления: Учебное пособие. – М.: Книжный дом «ЛИБРОКОМ», 2009, 304 с.
6. Парийская Е.Ю. Сравнительный анализ математических моделей и подходов к моделированию и анализу непрерывно-дискретных систем // Дифференциальные уравнения и процессы управления: электронный журнал, № 1, 1997, С. 91–102. URL: http://www.neva.ru/journal.
7. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. – М.: АСТ, 2006. – 504 с.
8. Поспелов Д.А. Ситуационное управление: теория и практика. – М.: Наука, 1986, 288 с.
9. Поспелов Д.А., Пушкин В.Н. Мышление и автоматы. – М.: Изд-во «Советское радио», 1972, 224 с.

УДК 004.65

SMARTY-ОБЪЕКТЫ В СИТУАЦИОННО-ОРИЕНТИРОВАННЫХ БАЗАХ ДАННЫХ

Головкин Юрий Борисович[1], Гусаренко Артем Сергеевич[2],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
[2]Уфимский Государственный авиационный технический университет,
Россия, г. Уфа, ул. К. Маркса, д. 12,
e-mail: comparif@rambler.ru.

Аннотация: В статье рассматривается динамическая модель более высокого уровня абстракции, для спецификации Smarty-объектов и рассматривается подключение нового типа гетерогенных источников JSON. Приводится в концептуальном виде модель компиляции шаблонов tpl. Примером для реализации предлагается использовать СОБД-ситуационно-ориентированные базы данных содержащих в своей основе динамическую модель.

Ключевые слова: *NoSQL; динамическая модель; JSON; Smarty; ситуационно-ориентированные базы данных.*

SMARTY-OBJECTS IN SITUATION-ORIENTED DATABASES

Golovkin Yury [1], Gusarenko Artem[2],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2]Ufa State Aviation Technical University,
Russia, Ufa, K. Marx str, 12,
e-mail: comparif@rambler.ru.

Abstract: The article considers the the dynamic model of higher level abstraction for the specification of Smarty- objects and connection of a new type of heterogeneous JSON-sources. Given in the form of a conceptual model of template compilation tpl. An example for the implementation of proposed use SOBD that is situationally-oriented databases comprises dynamic model.

Keywords: *NoSQL; dynamic model; JSON; Smarty; situation-oriented databases.*

В рамках ранее разработанной концепции модели DOM-элементов в составе динамической модели ситуационно-ориентированной базы данных предлагается динамическая модель более высокого уровня абстракции, предусматривающей графические и текстовые средства спецификации источников данных на основе JSON (JavaScript Object Notation). Описывается способ спецификации JSON источников с помощью JSON-элементов, ассоциированных с состояниями динамической модели, который регламентирует заполнение Smarty-объекта и/или Smarty-массива JSON-контентом из специфицированных источников, когда родительское состояние становится текущим. Предлагается реализация модели на платформе PHP с использованием tpl-шаблонов Smarty. Развивая концепцию ситуационно-ориентированных баз данных (СОБД) предложенную в работах [1-5], необходимо отметить, что в основу NoSQL баз данных [6-8] входят различные виды источников. Текущее положение дел таково, что базы данных имеют в своей структуре источники JSON типа, он представляет собой массив или объект данных и используется не только для информационного обмена между сервером и клиентом веб-приложения, а служит основой баз данных. Такой формат является дополнительным способом хранения данных на сервере, с его помощью можно описывать объекты и сложные иерархические структуры данных, но СОБД в своем наборе инструментов не имеют осязаемого подхода к подключению и обработке источников данного типа, а также алгоритмов, лингвистического обеспечения и встроенных средств вывода контента пользователю.

В качестве примера в данной статье приводится тестовый набор данных, с ситуациями «СписокСтудентов» и «ВыбранСтудент», концептуальные модели данных JSON-источника приведены на рис. 1. Суть примера заключается в отображении списка сдач по предмету выбранного студента. В примере участвуют три источника «список студентов», «список предметов», «список сдач». Задача состоит в извлечении данных из каждого источника по идентификаторам, таким как «код предмета» и «код студента». Идентификаторы присутствуют как в элементах, так и в атрибутах, обозначаемых ключевым словом JSON-нотации @attributes. Типовые операции извлечения данных записываются на языке динамической модели СОБД, для снижения рутины программирования. Как уже было отмечено в СОБД нет специальных средств для спецификации процедур извлечения, очистки и фильтрации JSON, относящегося к гетерогенным источникам данных, поэтому на рисунках 1 и 2 отображается решение данной проблемы в графической интерпретации модели СОБД. В исходной ситуации «СписокСтудентов» на экране отображается список студентов, сформированный из гетерогенного источника и представленный в виде радиокнопок. При этом компилируется отдельный шаблон tpl для каждой ситуации. Схема компиляции шаблона по отображению списка сдач выбранного студента приведена на рис.2. Если для XML баз данных для отображения контента

использовалась технология XSLT шаблонизации, то для JSON источников вопрос представления контента не останется открытым благодаря набравшему популярность шаблонизатору Smarty. Компилирующий обработчик шаблонов Smarty имеет базовые и расширенные возможности по отображению таких структур данных как массивы и объекты, создание шаблонов имеет структуру подобную PHP-программе, также как в JSON описание данных похоже на описание на JavaScript-программы.

В работах [9],[10] рассматривались различные аспекты использования источников XML и отображения динамического контента с помощью XSLT, но не рассматривались вопросы, связанные с JSON и Smarty как платформы СОБД. Это привело к тому, что сейчас нет специальных видов обеспечения для СОБД по работе с указанной функциональностью.

В данной статье рассматриваются вопросы автоматического формирования контента рис 1., из ассоциированных JSON-объектов и JSON-массивов с состояниями динамической модели СОБД, а также спецификации отображения с помощью Smarty в модели веб-приложения. Суть использования tpl-шаблонов заключается в формировании Smarty-объекта и доведение его до финального состояния содержания, требуемого контента, это означает, что в ситуации, когда все процедуры обработки завершены и контент доведен до уровня требуемого результата, происходит его вывод. Вывод результата в браузер клиента производится путем рендеринга объекта в шаблоне tpl. Шаблон tpl содержит спецификации на языке программирования php. Для интерпретатора в модели вместо stylesheet конструкции используется конструкция tpl рис. 2, в которой задается имя шаблона, который должен быть использован для отображения контента.

Метод tpl используется как альтернатива методу xslt для трансформации. Исходная ситуация содержит список студентов, среди которых выбирается нужный нам студент, для получения детальных сведений по сдачам и предметам. Список студентов сформирован на основе документа doc:СписокСтудентов. Для исходной ситуации «Студенты» предусмотрен шаблон tpl:СписокСтудентов. Шаблон компилируется, отображая каждого студента, концептуальная модель компиляции шаблона tpl:СписокСтудентов приведен на рис. 2.

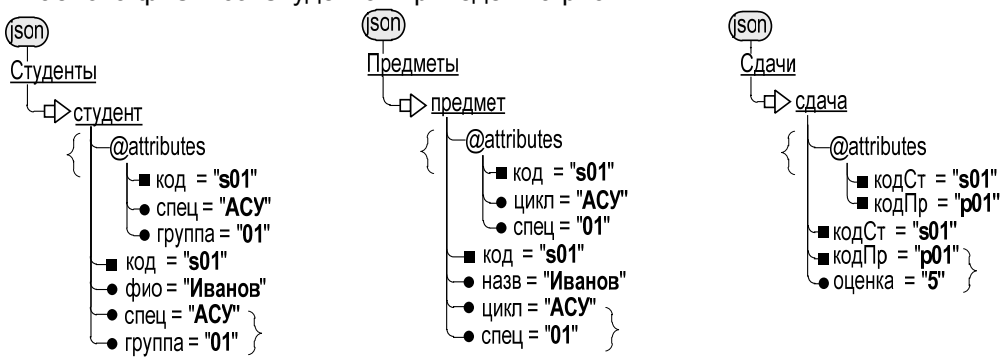


Рис. 1. Концептуальная модель данных JSON источника

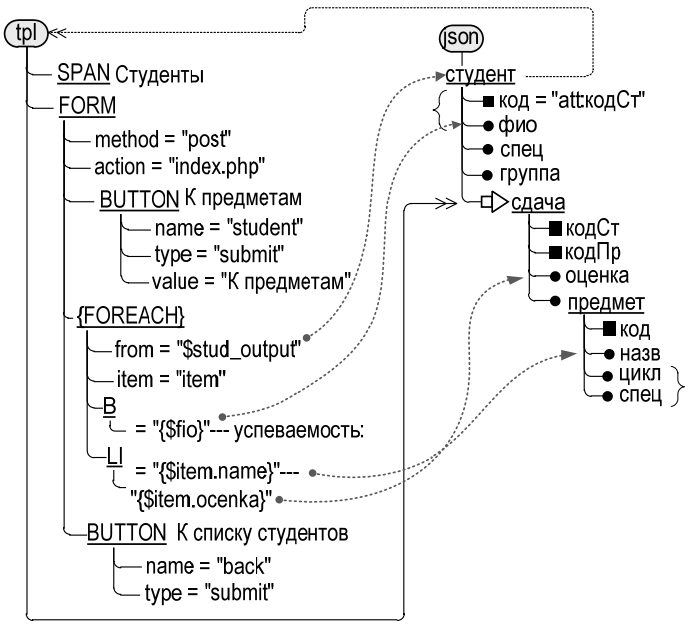


Рис. 2. Схема компиляции шаблона tpl в ситуации «ВыбранСтудент»

Код студента может быть выбран как из атрибутов, так и из свойств объекта «Студент». При выполнении каждой итерации цикла FOREACH шаблона добавляется элемент INPUT, который содержит идентификационные сведения каждого студента. Элемент INPUT имеет тип type="radio", что отображается браузером как набор радиокнопок, для выбора одного из студентов и кнопка BUTTON для перехода в следующее состояние «ВыбранСтудент» отражающее сведения об успеваемости выбранного студента, для этой ситуации предусмотрен шаблон tpl:УспеваемостьСтудента. Шаблон tpl:УспеваемостьСтудента отображает содержимое Smarty-объекта по выбранному студенту, концептуальная модель компиляции шаблона приведена на рис. 2. Результат компиляции второго шаблона «УспеваемостьСтудента» представляет собой список из элементов разметки LI сдач по каждому предмету отделенных от оценки по каждому предмету тройным знаком тире.

СПИСОК ЛИТЕРАТУРЫ

1. Гусаренко А. С., Миронов В. В., Ситуационно-ориентированные базы данных: концепция управления XML-данными на основе динамических DOM-объектов // Вестник УГАТУ: научн. журн. Уфимск. гос. авиац. техн. ун-та. 2012. Т.16, №3 (48). С.159–172.
2. Гусаренко А. С., Миронов В. В. Динамические DOM-объекты в ситуационно-ориентированных базах данных: лингвистическое и алгоритмическое обеспечение источников данных // Вестник УГАТУ: научн. журн. Уфимск. гос. авиац. техн. ун-та 2012. Т. 16, № 6 (51). С. 167–176.
3. Гусаренко А. С., Обработка XML-документов в ситуационно-ориентированных базах данных на основе динамических DOM-объектов // автореферат диссертации на соискание ученой степени кандидата технических наук / Уфимский государственный авиационный технический университет. Уфа, 2013
4. Гусаренко А. С., Управление XML-данными на основе динамических DOM-объектов // Перспективы развития информационных технологий: сб. мат. 6-й междунар. науч.-практ. конф. Новосибирск: Сибпринт, 2011. С. 103–108.
5. Головкин Ю.Б, Миронов В.В., Ахметшин Р.Ф. Концепция объектно-ориентированных иерархических ситуационных моделей автоматизированного управления. Управление сложными техническими системами. Межвуз. науч.сб. - Уфа, УГАТУ, 2000.
6. Гусаренко А. С., Миронов В. В. Управление XML-данными с помощью динамических DOM-объектов в ситуационно-ориентированных базах данных // Модернизация современного общества: пути развития и перспективы: матер. 2-й междунар. науч.-практ. конф. Ставрополь: ЦНЗ "Логос", 2011. С. 38–43. (опубл. на англ. яз.)
7. Гусаренко А. С., Миронов В. В. Ситуационно-ориентированные базы данных: концепция управления XML-данными основанная на динамических DOM-объектах // Труды 14-й междунар. конф. по выч. наукам и инфор. техн. (CSIT'2012). Уфа-Гамбург-Норвежские Фьорды, 2012. Т. 1. С. 61–67. (опубл. на англ. яз.)
8. Гусаренко А. С., CRUD-операции в ситуационно-ориентированных базах данных на основе динамических DOM-объектов // Повышение эффективности использования информационных технологий в государственном и муниципальном управлении: матер. всерос. науч.-практ. конф. с участием междунар. представителей. Уфа: БАГСУ, 2012. С. 34–37.
9. Головкин Ю.Б.,Гусаренко А.С., Моделирование производственных систем в GPSS // Межв. сб. науч. тр.: Управление в сложных системах. Уфа: УГАТУ, 2011. С. 136–150.
10. Головкин Ю.Б., Гусаренко А.С., Информационная система кредитования юридических лиц в банке // Актуальные инновационные исследования: наука и практика. 2010. № 3. С. 14.

УДК 681.51

ДИНАМИЧЕСКАЯ МОДЕЛЬ ДИСКРЕТНЫХ ПРОЦЕССОВ С УЧЕТОМ ПРЕДЫСТОРИИ

Головкин Юрий Борисович[1],Ярцев Рустем Альбертович[2], Газетдинова Светлана Геннадьевна[3],Арсланова Айгуль Римовна[4], Давлетов ГазимБатырович[5],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
[2,3,4,5]Уфимский Государственный авиационный технический университет,
Россия, г. Уфа, ул. К. Маркса, д. 12,
e-mail: comparif@rambler.ru.

Аннотация: Рассматривается проблема контроля текущего состояния дискретного процесса с учетом предыстории. Для ее решения предлагается учитывать в динамической модели процесса возможные внутренние состояния.

Ключевые слова**:** *процесс; модель; граф; метод; состояние.*

DYNAMIC MODEL DISCRETE PROCESSES WITH HISTORY

Golovkin Yury [1], Yarchev Rustem[2], Gazetdinova Svetlana [3], Arslanova Aigul[4], Davletov Gazim[5],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg,Sadovaya str., 21,
[2,3,4,5]Ufa State Aviation Technical University,
Russia, Ufa, K. Marx str, 12,
e-mail: comparif@rambler.ru.

Abstract:*Considered in the article problem control state discrete process with history. For decider propose registration in the dynamic model process internally states.*

Keywords: *process; model; graph; method; state.*

Как известно, многие процессы, протекающие в сложных системах, носят дискретный характер, т.е. характеризуются множеством различных состояний, в каждом из которых поведение процесса качественно не изменяется до наступления некоторого события, определяющего переход в другое состояние. Следовательно, описание такого процесса будет неполным, если не задать еще множество всех имеющихся переходов между состояниями, а также условия этих переходов, связанные с наступлением различных событий. Кроме того, нужно учесть возможность конфликта переходов, условия которых выполнены для текущего состояния процесса одновременно, а также предусмотреть обеспечение оператора, контролирующего ход процесса, всей необходимой информацией.

Данные процессы составляют основу более сложных динамических структур, связанных с управлением объектами любой предметной области, поэтому для каждого из них введено понятие элементарного процесса (ЭП) [1]. Контроль поведения ЭП во времени может быть осуществлен при помощи конечного автомата Мура на основе моделей, представляющих контролируемый процесс в виде графа и получивших название статических [2]. При этом функционирование данного автомата в каждый момент контроля ***t*** может быть описано следующим образом:

1. При помощи процедуры поиска символов во входном слове автомата X(t), описывающем условия всех переходов, которые выполнены в момент t, определяется текущее значение предиката активности ЭПра(t)(т.е. фиксируется наступлениесоответствующего внешнего события или событий): если ра(t)=1, то процесс в данный момент считается активным, если же ра(t)=0 – то пассивным.

2. Если ЭП активен, то автомат на основе статической модели М и входного слова X(t) строит динамическую модель М(t), которая включает текущую вершину s(t), изображающую состояние ЭП в момент t, а также выходное слово процесса Y(t), несущее информацию о ходе его развития в данный момент. При этом вершина s(t) хранится в памяти автомата до следующего момента контроля t+1, а слово Y(t) предоставляется управляющему для принятия решения.

3. Если ЭП пассивен, то на устройство отображения передается слово Y(t)=Y0, информирующее управляющего о пассивности контролируемого ЭП, а вершина s(t) не определяется.

Недостаток такого подхода состоит в том, что развитие управляемого процесса в каждый момент t зависит только от внешних условий, описанных во входном слове X(t), и от состояния s(t-1), на котором остановилось развитие ЭП в предыдущий момент t-1, поскольку сама модель М инвариантна ко времени, а при построении из нее модели М(t)начальная вершина σ (t) определяется следующим образом:

$$\sigma(t) = \begin{cases} s(t-1), \text{если } p_a(t-1)=1, \\ \sigma, \text{ в противном случае.} \end{cases} \quad (1)$$

Здесь σ - начальная вершина статической моделиМ [1, 2].

Между тем развитие ЭП в момент t может также зависеть и от предыстории поведения этого процесса в предшествующий момент t-1, поскольку состояние s(t-1)=σ (t) может наступить в различных режимах управления процессом. Следовательно, при указанных обстоятельствах известные модели М и М(t)перестают быть адекватными описываемому ими процессу, что обуславливает невозможность их применения при построении АСУ такими ЭП.

Возникает задача усовершенствования моделирования и контроля ЭП с учетом предыстории, которая может быть решена следующим образом.

Во-первых, каждая дуга dk графа ЭП G, составляющего основу модели М, помимо строки символов c(dk,G)алфавита C, несущей информацию о развитии процесса для оператора (это может быть также пустая строкаc0), дополняется строкой c’(dk,G)алфавита C’, которая используется для внутренней обработки соответствующих данных автоматом. При этом в частном случае C = C’ и c(dk,G) = c’(dk,G).

Во-вторых, внешнее условие активности дуги dk, связывающее переход ЭП с наступлением некоторых внешних событий, дополняется через логическое «ИЛИ» внутренним условием, задающим возможность перехода по данной дуге в зависимости от того или иного внутреннего события. При этом к числу внутренних событий могут быть отнесены последовательности состояний и переходов ЭП, которым соответствуют определенные вершины и дугиG. Все внутренние события также описываются символами алфавита C’.

В-третьих, статическая модель М дополняется рекурсивной функцией внутреннего информационного сопровождения вида y = e’(G), формирующей некоторое слово как результат сцепления символовc’(dk,G) тех дуг графа G, которые соответствуют пути развития ЭП.

Введенные дополнения позволяют формировать в каждый момент времени t внутреннее выходное слово автомата Y’(t) = e’(G(t)), где G(t) – активный надграфG, содержащий только активные дуги и соответствующие им вершины [3],[4]. Данное слово передается на следующий такт работы автомата в качестве внутреннего входного слова X’(t+1), т.е. X’(t+1) = Y’(t), и далее шаги 1-2 работы автомата выполняются с использованием комбинированного входного словаX*(t+1) = X(t+1) ’’ X’(t+1),

где ’’ – операция конкатенации или сцепления символов. В самый же первый момент времени комбинированное входное слово X*(1)будет совпадать с внешним словом X(1), т.е. определяться наступлением исключительно внешних событий.

Таким образом, все возможные динамические модели M(t), формируемые на основании статической модели M и комбинированного входного слова X*(t), будут учитывать предысторию развития ЭП уже не только путем формирования исходной вершины σ (t), но и через построение самого активного надграфаG(t). Предлагаемое новшество может быть использовано как для усовершенствования уже известных моделей дискретных процессов (см., например, [5],[6],[7]), так и для моделирования тех систем, в которых данная методология еще не применялась [8],[9].

СПИСОК ЛИТЕРАТУРЫ

1. Ярцев Р.А. Об автоматизации управления элементарными процессами в сложных системах. Рукопись деп. в ВИНИТИ, 13.02.91, № 739-В91. 29 с.
2. Виссарионов В.С., Головкин Ю.Б., Газетдинова С.Г., Ярцев Р.А. Об алгоритме контроля простого элементарного процесса. Рукопись деп. в ВИНИТИ, 24.05.06, № 703-В2006. 11 с.
3. Миронов В.В., Головкин Ю.Б., Юсупова Н.И. Об автоматной модели динамической ситуации // Управление сложными техническими системами: межвуз. науч. сб. №9. Уфа: УАИ, 1986. С. 3-10.
4. Газетдинова С.Г., Ярцев Р.А. О построении моделей управления на основе графов с приоритетами по методологии экспертных оценок // Вестник УГАТУ.- Уфа: УГАТУ, 2006 - Т.7, №2 (15). - С.212-222.
5. Миронов В.В., Ярцев Р.А. Об автоматизации управления иерархическими процессами в сложных системах. Рукопись деп. в ВИНИТИ, 30.09.91, № 3822-В91. 83 с.
6. Головкин Ю.Б., Гусаренко А.С., Информационная система кредитования юридических лиц в банке // Актуальные инновационные исследования: наука и практика. 2010. № 3. С. 14.
7. Головкин Ю.Б.,Гусаренко А.С., Моделирование производственных систем в GPSS // Межв. сб. науч. тр.: Управление в сложных системах. Уфа: УГАТУ, 2011. С. 136–150.
8. Кромина Л.А., Ярцев Р.А.Формирование заказа литературы для библиотеки вуза на основе локальных рейтингов изданий как задача исследования операций // Вестник УГАТУ.- Уфа: УГАТУ, 2010 - Т.14, №5 (40). - С.176-187.
9. Миронов В.В., Ярцев Р.А., Кромина Л.А. Применение общих рейтингов заказываемых изданий при формировании оптимального варианта заказа литературы для вуза // Вестник НГУ. Серия: информационные технологии: научн. журн. Новосиб. гос. ун-та, 2012. Т. 10, №4. С. 5-12.

УДК 004.056.5

АНАЛИЗ СОСТОЯНИЯ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ОТЕЧЕСТВЕННЫХ СИСТЕМАХ ЗАЩИТЫ И ИХ СРАВНЕНИЕ

Дубровская Виктория Андреевна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д.67,
e-mail: torry_2902@mail.ru

Аннотация: В России создаются и используются различные системы защиты информации. С целью создания общей картины о состоянии используемых средств защиты информации в отечественных системах защиты был проведен сравнительный анализ разноплановых отечественных систем защиты информации. В статье представлена сравнительная таблица, в которой приведен список основных каналов утечки и кражи информации и перечислены способы и средства противостояния злоумышленникам, которые используются в отечественных системах защиты информации. Эти данные помогли сформировать представление о состоянии используемых средств защиты информации в России, а так же выявить сильные и слабые стороны отечественных систем.

Ключевые слова*: системы защиты информации; каналы утечки информации; средства защиты информации; безопасность.*

ANALYSIS OF THE USED INFORMATION SECURITY FEATURES IN DOMESTIC PROTECTION SYSTEMS AND THEIR COMPARING

Victoria Dubrovskaya,
The St. Petersburg State University of aerospace instrumentation,
Russia, St. Petersburg, Bolshaya Morskaia str. 67,
e-mail: torry_2902@mail.ru

Abstract: In Russia different systems of information security are created and used. For the purpose of creation of an overall picture about a status of the used information security features in domestic systems of protection the comparative analysis of versatile domestic systems of information security was carried out. There is the comparative table, in which the list of the main channels of leak and theft of information is provided and methods and funds of opposition to malefactors, which are used in domestic systems of information security, are transferred. These data helped to create view of a status of the information security features used in Russia and also to reveal the strengths and weaknesses of domestic systems.

Keywords: *systems of information security; channels of information leakage; information security features; security.*

На протяжении всей мировой истории информация играла важную роль в развитии человечества. Факт владения даже малой её долей мог изменить ход событий и становился решающим во многих политических, экономических и военных ситуациях. Поэтому вопрос защиты информации остро стоял даже во времена Цезаря, который придумал один из первых алгоритмов ее шифрования с целью защиты.

В современном мире, при прогрессивном переходе от материального метода хранения информации к электронному виду, особое внимание следует уделить используемым средствам защиты информации, как от несанкционированного доступа, так и от нежелательных утечек и уничтожения важных данных. Для обеспечения информационной безопасности в процессе ведения бизнеса и создания нового отечественного программного продукта следует провести анализ систем защиты информации и положения дел в области информационной защиты в России.

В настоящий момент из-за стремительного роста прогресса в области информационных технологий соответствующее обучение людей дисциплинам, связанным с информатикой и информационной безопасностью, является способом воспитания ответственного, более внимательного отношения к информации и её защите. Активное распространение использования информационных технологий во всех сферах деятельности людей обуславливает практическую необходимость человека, как сотрудника, и как рядового пользователя, обучаться способам безопасной работы с информацией и методам ее защищенной обработки. Поэтому задача эффективного обучения технических специалистов в области информационных технологий становится насколько необходимым, настолько сложным, многогранным и продолжительным процессом.

Система подготовки в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образовательной деятельности, как общего: пропедевтика, базовый и профильные курсы информатики, так и профессионального: среднего, высшего, послевузовского и дополнительного образования. При этом роль общего образования является основополагающей, поскольку в процессе информационной подготовки на этапе общего образования закладываются основы компьютерной грамотности и компетентности как фундамент информационной культуры личности [1]. Связь между общим и профессиональным образованием удачно регулируется введением и использованием компетентностного подхода.

Компетентностный подход реализует методологические, организационные, содержательные, дидактические и технологические аспекты, делает главным участником образовательного процесса именно студента, с его индивидуальными целями и задачами. Данный подход позволяет направить педагогическую деятельность на вовлечение студента в активную, осознанную деятельность, на развитие информационных, коммуникативных, учебно-познавательных компетенций и развитие личностного потенциала студента, формирование самооценки, самоконтроля студентов и рефлексии педагога, которая позволяет добиваться лучших результатов [2].

Для обеспечения более полного и подробного представления об информационной защите обратимся к ГОСТ Р 50992-2006 «Защита информации. Основные термины и определения» [4] и напомним основные необходимые понятия, термины и определения:

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Защита информации от несанкционированного воздействия – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность безопасности информации.

В Федеральном законе от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» отмечено:

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации [7].

– Возможными последствиями некачественно организованной защиты информации являются:

– утечки персональных данных сотрудников компании и организаций-партнеров;

– раскрытие коммерческой тайны и ноу-хау;

– открытый доступ к служебной переписке;

– несохранение государственной тайны;

– полное либо частичное лишение работоспособности системы безопасности компании [5].

Утечки можно так же разделить по характеру появления на случайные, допущенные работником фирмы по неосторожности, незнанию или неосведомленности, и на умышленные [6].

К умышленным утечкам относятся заранее организованные и специально реализованные воздействия с целью спланированного кражи или уничтожения определенной информации, то есть пользователь, работающий с информацией, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду. Также утечки информации могут классифицироваться в зависимости от используемых злоумышленником каналов – сложные сценарии или действия пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы, в результате выполнения которых потерян контроль над информацией, нарушена ее конфиденциальность [6].

Российской компанией InfoWatch, ведущей глобальные статические исследования утечек информации в мире, было опубликовано распределение случайных и умышленных утечек информации за первое полугодие 2014 года (рисунок 1) [6].

Рис. 1. Распределение случайных и умышленных утечек по каналам за первое полугодие 2014 года

По данным компании InfoWatch процентное соотношение случайных и умышленных утечек практически равно 50 на 50 [6]. Это говорит о том, что средства защиты информации и способы построения информационной безопасности должны фокусироваться не только на подготовленных злоумышленников, но и обеспечивать защиту от неосведомленных случайных действий.

Из данных рисунка 1 видно, что процент неопределенных умышленных утечек наивысший, что сигнализирует о том, что при использовании программно-аппаратных комплексов средств защиты информации нужно организовывать пытливый аудит с целью определения хотя бы способа кражи информации для последующего повышения ее защищенности. Повышение степени защиты от случайных и умышленных утечек информации возможно ещё за счёт как можно более точного определения места и времени утечки, и выявления конкретного оператора или сотрудника.

В распределении случайных утечек информации можно выделить, например, утечки информации через электронную почту. Скорее всего, они обусловлены невнимательностью оператора при вводе почтового адреса, или при выборе прилагаемого документа. То есть сама информация, циркулирующая в электронной почте, также должна быть защищена шифрованием.

Внушающим по своему использованию еще является такой канал утечки, как бумажные носители, то есть кража и уничтожение информации, хранящейся на бумажных носителях и «твердых» копиях.

Для обеспечения общей безопасности в организациях и на предприятиях заботящихся о сохранности своей информации принято использовать различного рода программно-аппаратные комплексы средств защиты информации в разумном сочетании с организационными мероприятиями и дисциплиной, так как основной причиной утечки информации является человек.

При всём этом надо понимать, что абсолютную защиту создать невозможно. Однако существуют основные принципы, необходимые при создании и работе систем защиты данных:

– полнота контроля процессов обработки информации – комплексность;
– подстраиваемость к изменяющимся условиям – адаптируемость;
– согласованность функций между элементами системы защиты – системность.

Только построенные по этим принципам системы защиты информации способны снизить вероятности утечки информации до должного уровня и обеспечить необходимую безопасность в организациях и на предприятиях.

Учитывая приведенный на рисунке 1 список каналов утечки, была составлена таблица 1, в которой проведен анализ некоторых систем защиты информации российских производителей. Для каждого канала утечки информации определяются определенные способы осуществления несанкционированного доступа к данным и ставятся в противодействия возможные и самые распространяемые способы защиты. Таким образом, в последнем столбце таблицы указаны российские системы защиты информации, которые обладают определенными в столбце «противодействие» средствами защиты информации.

Таблица 1

Возможности противодействия различных российских систем защиты информации действиям злоумышленников в зависимости от используемого канала утечки информации

Канал		**Специфика использования канала**	**Противодействие**	**Программно-аппаратные продукты**
№	**Наименование**			
1	Кража или потеря оборудования	«Уборка мусора»	Гарантированное затирание данных Гарантированное удаление информации Оба варианта должны автоматически производить «зачистку» оперативной памяти, временных файлов	Secret Net Dallas Lock Панцирь Secret Disk
		Хищение оборудования или доступ к нему	Информация на дисках должна храниться в шифрованном виде Лучшим вариантом считается и работа с дисками и информацией в режиме прозрачного кодирования	Dallas Lock Панцирь ГРИМ-ДИСК Secret Disk
		Создание поддельных ключей и кража паролей	Хранилище паролей и электронных ключей должно находиться на аппаратной составляющей Храниться должны не сами пароли, а их хеш-функции, лучше всего в шифрованном виде	Secret Net Dallas Lock Панцирь Аккорд
2	Мобильные устройства		(системы MDM)управление мобильными устройствами, позволяющими удаленно обновлять, конфигурировать и очищать устройства	mobilEcho MobileIron Good Technology
		«Уборка мусора»	Гарантированное затирание данных Гарантированное удаление информации Оба варианта должны автоматически производить «зачистку» оперативной памяти, временных файлов	mobilEcho
			ЭЦП Шифрование ЗПС – программы, которые можно открывать те или иные файлыаудит	mobilEcho MobileIron
			Удаленная блокировка и полная очистка устройств Выборочное удаление данных	mobilEcho MobileIron McAfee Enterprise Mobility Management
3	Съемные носители		Регистрация их в системе Разрешение работы только с зарегистрированными внутрифирменными флешками и прочим	Secret Net Dallas Lock
		Загрузка сторонней ОС с внешних носителей	Аппаратных доверительных загрузчик. Программные средства (обычно менее действенные, чем аппаратная составляющая)	Secret Net Dallas Lock Панцирь Аккорд Электронный замок «Соболь»

4	Сеть (браузер, Cloud)	Перехват во время передачи данных	Шифрование трафика	Панцирь
		Вирусы, вредоносные программы, троянский конь и прочее	Формирование ЗПС Контроль целостности конфигурации системы, ее компонентов, определенных файлов Возможность восстановление конфигурации Периодичная архивация нужной (важнейшей) информации	Secret Net Dallas Lock Панцирь Аккорд Электронный замок «Соболь» Криптон-Замок
5	Электронная почта		Наличие межсетевых экранов, прокси-серверов Использование электронно-цифровых подписей	TrustAccess Cisco Secure PIX Firewalls
		Перехват во время передачи данных	Шифрование трафика	Панцирь
6	Бумажные документы	Вывод информации на печать	Регистрация и учет работы пользователя Маркировка всех отпечатанных страниц Теневое копирование Регистрация, контроль и доступ к внешним устройствам	Secret Net Dallas Lock Аккорд
7	IM (текст, голос, видео)	Кража времени и установка игровых программ	Формирование ЗПС Учет и регистрация работы пользователя	Secret Net Dallas Lock Панцирь Аккорд
8	Не определено		Учет и регистрация работы пользователей	Secret Net Dallas Lock Панцирь Криптон-Замок
			Идентификация и аутентификация пользователей	Электронный замок «Соболь» Secret Net Dallas Lock Панцирь Аккорд Криптон-Замок UMATCH BioLink Mouse EyeD Opti Mouse ruTocken MemoryTouch

В результате проведённого анализа установлено практически равное распределение случайных и умышленных утечек информации. Это подтверждает то, что для защиты информации следует учитывать, как правильное и эффективное использование систем защиты информации, так и степень образованности и моральности персонала. Поэтому помимо технических средств защиты не стоит пренебрегать и работой с персоналом, с их головами, умами, создавать такие условия, чтобы не возникало желания в хищении информации. Помимо работы с персоналом на каждом отдельно взятом предприятии, необходимо в общеобразовательных учреждениях уделять должное внимание воспитанию у молодёжи трепетного и ответственного отношения к информации.

А технические средства должны обеспечивать сохранность и целостность данных, затруднять попытки утечки и кражи информации, обеспечивать неотвратимость наказания за хищения уже только тем, что тайное всё равно станет явным. Средства защиты с большой вероятностью должны указать злоумышленника, для чего должен быть развит и настроен пытливый аудит и подробный мониторинг.

Таким образом, система защиты информации это не случайный набор функций, а системные программно-аппаратные комплексы, охватывающие целый перечень задач по защите информации. Однако по данным приведенным в Таблице 1 видно, что не все каналы утечки информации могут быть охвачены одной, универсальной системы защиты. Отсюда следует, что для качественной защиты своего бизнеса или какой-либо конфиденциальной информации необходимо для начала досконально изучить и рассмотреть используемые средства хранения, передачи и обработки информации, чтобы подобрать в соответствие с ними правильные и действенные методы защиты. Определить подходящую систему или комплекс систем из существующих, или же, если этого недостаточно, то стоит заказать разработку новой, чтобы она учитывала специфику ведения бизнеса в конкретной организации. Однако это достаточно затратное мероприятие как финансово, так и по времени. Так как пока разрабатывается система защиты информации, бизнес должен вестись и развиваться. В это время меняются приоритеты его ведения, способы его организации и поддержки, развивается технологический прогресс, что пагубно отражается на развитии как самого бизнеса, так и новой системы защиты информации в целом. Поэтому, исследуя известные системы защиты информации и выявив их общие слабые места, можно создать дополнительные модули или отдельные надстройки, которые будут более качественно защищать информацию, перекрывать практически все «дыры» данного канала и возможные способы утечки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Кошелева С.Б. Начальная подготовка обучающихся в области информационной безопасности // Проблемы и перспективы развития образования в России – 2011, №11, С.156–160.
2. Кошелева С.Б. Компетентностный подход как условие непрерывности в обучении основам информационной безопасности. //Вестник Костромского государственного университета им. Н.А. Некрасова. Серия: Педагогика. Психология. Социальная работа. Ювенология. Социокинетика. – 2012, Т.18, №4, С.83–86.

3. Степанов А.Г. Вопросы информационной безопасности в непрерывной системе обучения информатике // Безопасность информационных технологий, 2005, №1, С.62–66.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
5. Несанкционированный доступ [Электронный ресурс] – режим доступа https://ru.wikipedia.org/wiki/Несанкционированный_доступ
6. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2014 года // Аналитический центр InfoWatch. 2014, 21с.
7. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и информационных технологиях и о защите информации».
8. Crypton Lock [Электронный ресурс] – режим доступа http://www.rutoken.ru/products/all/crypton-lock/
9. СЗИ от НСД Secret Net [Электронный ресурс] – режим доступа http://www.securitycode.ru/products/secret_net/ (Дата обращения: 06.04.2014).
10. DALLAS LOCK – Система защиты информации от несанкционированного доступа [Электронный ресурс] – режим доступа http://www.dallaslock.ru/ (Дата обращения: 06.04.2014).
11. СЗИ НСД «Аккорд-АМДЗ» [Электронный ресурс] – режим доступа http://www.accord.ru/accord.html (Дата обращения: 06.04.2014).
12. Комплексная система защиты информации «ПАНЦИРЬ-К» для ОС MICROSOFT WINDOWS [Электронный ресурс] – режим доступа http://npp-itb.spb.ru/products/nsdk.shtml (Дата обращения: 06.04.2014).
13. Дмитриев А. Системы защиты информации. //Мир ПК. 2001, №05.
14. Щеглов А.Ю. КСЗИ «Панцирь-К» для ОС Windows 2000/XP/2003 – оптимальное решение для защиты конфиденциальной информации и персональных данных // Защита информации.

УДК 004.056.53

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ЛАЗЕРНЫМ МИКРОФОНАМ

Золотарева Ксения Николаевна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, д.49,
e-mail: ksenya2894@rambler.ru

Аннотация: В статье рассмотрены основные организационные методы защиты информации от негласного съема с помощью лазерного микрофона, особенности выполнения организационных мероприятий и анализ размера затрат на защиту информации.

Ключевые слова: *лазерный микрофон, организационные методы, информационная безопасность.*

ORGANIZATIONAL METHODS TO COUNTERACT LASER MICROPHONES

Zolotareva Ksenya,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverskyaya Street 49,
e-mail: ksenya2894@rambler.ru

Abstract: The article describes the main organizational methods to protect information from covert eavesdropping using a laser microphone, especially the performance of organizational activities and analysis of costs.

Keywords: *laser microphone, organizational methods, information security.*

Введение. Организационные меры защиты также немаловажны и позволяют повысить возможность 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. Исходя из этого, можно выделить следующие организационные методы противодействия лазерным микрофонам [1] YANDEX_8:

– использование погодных и климатических условий (дождь, снег, сильный ветер и т.д.);

– ведение переговоров в местах с высоким уровнем фоновых шумов (как внешних, так и внутренних);

– фоновый шум будет влиять на качество перехваченной информации;

– размещение на местности таким образом, чтобы на пути распространения лазерного луча были естественные и искусственные препятствия (кустарник, строения и т. д.);

– использование зеленых насаждений. Любые препятствия будут затруднять возможность наводки лазера на окно, создавая сложности в выборе точки съема и расположения аппаратуры на местности;

– использование недоступных для лазерного подслушивания помещений (окна выходят во двор; подвальные, полуподвальные помещения);

– увеличение расстояния до границы контролируемой территории;

– контролируемая территория – это пространство или территория, в пределах которой исключено неконтролируемое пребывание посторонних лиц [2]. За пределы данной территория информационные активы не должны уходить;

– расположение рабочих мест, исключающих прохождение акустических сигналов к окнам. Это рабочие места, как можно больше удаленные от окна, желательно огражденные специальными ширмами или шкафами. Ограждающие конструкции, мебель и другие предметы интерьера следует отодвинуть от стен и окон [3];

– использование аппаратуры предупреждения о применении лазерных систем;

– ведение переговоров, не повышая голоса, не срываясь на крик (разница в уровне речи между нормальным и громким голосом может достигать 15 дБ);

– увеличение расстояния от говорящего до окна.

К применению организационных мероприятий необходимо подходить разумно. Следует уделять особое внимание помещениям, в которых проводятся важные совещания, переговоры, конференции. Лучше их проводить в помещениях, где отсутствуют окна, что ликвидирует возможность негласного съема информации с помощью лазерных систем. В случае если нет такой возможности желательно предварительно выявить и локализовать уязвимые места – помимо окон это также любые другие отражающие поверхности, например, полированные предметы, остекления картин и портретов.

Также нельзя забывать и про режимные средства, которые обеспечивают порядок допуска и доступа людей в то или иное помещение. Использование всех вышеперечисленных методов может оказаться бесполезным, если комната переговоров не будет защищена от физического проникновения, в том числе и своих сотрудников. Нельзя допустить, чтобы это помещение превратилось в «проходной двор». Доступ в него должен быть ограничен. Кроме того, после и перед каждым значимым мероприятием должна проводиться быстрая проверка помещения [4].

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. На переговорах достаточно положить включенный диктофон с совмещенной записью между вами и собеседником, и у злоумышленника возникнут серьезные проблемы с пониманием сути переговоров, не говоря уже о том, что будет довольно сложно просто разобрать слова. В качестве зашумления можно использовать и звуковой фон помещения с большим количеством людей.

Значительные трудности для злоумышленника создаст непредсказуемость действий объекта наблюдения. Во время важного совещания откройте окна – это затруднит перехват отраженного луча, или же меняйте положение окна каждые 5–10 минут. Если у злоумышленника нет времени на подготовку места для подслушивания, то это усложнит съем информации.

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 (более 10тыс.USD), например, лазерный микрофон Laser-3000 стоимостью $51,495.00. Кроме того, требуется специальное обучение и использование компьютерной обработки речи для увеличения дальности. Наряду с зарубежными существует опытная отечественная система ЛСТ-ЛА2 с дальностью съема менее 100 м, но с достаточно скромной стоимостью. Что касается правовых аспектов, связанных с использованием лазерных микрофонов, стоит отметить, что они относятся к средствам негласного съема информации, которые внесены в «Список видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» утвержденный постановлением Правительства РФ № 214 от 10 марта 2000г. (с изменениями от 19 октября 2000 г., 27 ноября 2006 г., 14 февраля 2009 г., 8 декабря 2010 г).

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.

Если нет возможности создать полноценную защиту от действия лазерных систем, то следует ограничиться применением некоторых средств защиты и мероприятий. Ниже в таблице 1 показаны бюджетные и дорогостоящие средства защиты информации (СЗИ) от негласного съема речевой информации с помощью лазерных микрофонов, которые были упомянуты в качестве примера.

Таблица 1

Средства защиты информации разных стоимостных категорий

Бюджетные СЗИ	Дорогостоящие СЗИ
Генератор виброакустического шума ЛГШ-403 6 000 руб.	Генератор виброакустической защиты помещений VNG-012GL – 45 000 руб.
Архитектурная пленка Llumar R 20 SR CDF 300 руб./метр квадратный	Плёнка Llumar R 15 GO SR HPR 550 руб. за погонный метр

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. Если существует реальная угроза, защиту следует организовать с учетом особенностей расположения и функционирования объектов, с учетом технических и финансовых возможностей противостоящей стороны, а также с соблюдением требований по экологии, эргономике и эстетике [5]. Правило, которым следует руководствоваться при организации защиты: затраты на защиту информации не должны превышать цену защищаемой информации.

Заключение. 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 (в основном эргономических и стоимостных) 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.

Для обеспечения защиты информации от негласного съема с помощью лазерных микрофонов необходимо применять комплекс мер, которые включают в себя применение технических средств активной и пассивной защиты, а также выполнение организационных мероприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – Спб.: ООО «Издательство Полигон», 2000. – 856 с.
2. Специальные требования и рекомендации по технической защите конфиденциальной информации. Решение Коллегии Гостехкомиссии России. – 2001-03-02. – М.: Гостехкомиссии России, 2001. – № 7.2, 49 с.
3. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. – Москва: Издательство «НЕЛК», 2001. – 139 с.
4. Средства защиты речевой информации: [Электронный ресурс]. 2015. Режим доступа: http://confident.org.ua/index.php/stati-po-teme/175-sredstva-zashchity-rechevoj-informatsii.html/. (Дата обращения: 05.09.2015).
5. А.А. Хорев. Средства акустической разведки: направленные микрофоны и лазерные акустические системы разведки: // Спецтехника и связь. 2008. № 3. Режим доступа: http://www.analitika.info/info1.php?page=2&full=block_article55/. (Дата обращения: 11.09.2015).

УДК 519.688

АНАЛИЗ РЕАЛИЗАЦИЙ ПРОЦЕДУР ТИПИЗАЦИИ И ЭКСТРАПОЛЯЦИИ СИТУАЦИЙ В АЛГОРИТМЕ КЛАССИФИКАЦИИ СИТУАЦИЙ

Ковалев Илья Гаврилович,
Санкт-Петербургский государственный университет телекоммуникаций,
им. проф. М. А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков, д 22, к.1,
e-mail: mail.kovalev@gmail.com.

Аннотация: рассмотрено рекурсивное применение метода ситуационного управления к задаче классификации ситуаций в инфокоммуникационных системах, предложен алгоритм классификации ситуаций и проведен анализ реализаций ключевых шагов алгоритма.

Ключевые слова: *алгоритм классификации; ситуационное управление; типизация; частные показатели эффективности.*

ANALYSIS IMPLEMENTATIONS PROCEDURES TYPING AND EXTRAPOLATION SITUATIONS IN THE ALGORITHM OF CLASSIFICATION SITUATIONS

Kovalev Ilya,
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov, 22-1,
e-mail: mail.kovalev@gmail.com.

Abstract: considered the recursive application of situational control method to the problem of situations classification in information and communication systems, the algorithm of situations classification and the analysis of the key steps in algorithm implementations.

Keywords: *the classification algorithm; situational management; typing; private performance indicators.*

Введение. Анализ систем связи, в том числе специального назначения, обнаружил множественность и разнородность проявлений систем связи, выражающихся в наличии в рамках одной системы большого числа разнородных подсистем: изделий, трактов, служб, профилей, протоколов, платформ, сетей, соподчиненных систем. Каждое подобное проявление системы, как правило, связано с полезностной интерпретацией системы ЛПР, что, с учетом требований по полноте и непротиворечивости управления, порождает задачу управления интерпретациями системы связи в зависимости от сложившейся измеримой обстановки.

Практически это зачастую выражается в виде множества показателей (до нескольких десятков), эвристическое знание о взаимосвязях между которыми позволяет ЛПР принимать решения по управлению. Как правило, этими показателями являются частные (по характеризуемому проявлению системы связи) показатели эффективности (ЧПЭ), позволяющие сравнивать между собой разнородные системы. Необходимость в обоснованном принятии решений требует экспликации связей между этими показателями и механизмов выбора этих связей из множества возможных в конкретной измеримой обстановке, что позволяет рассматривать задачу классификации ситуаций в признаковом пространстве ЧПЭ.

Постановка задачи. Порождающим множеством ЧПЭ выступает МОТ-модель [1], определяющая множество интерпретаций системы связи, объединенных в признаковом пространстве, образованном шкалами наименований, соответствующих организационной, функциональной и логической декомпозиции системы связи (Рисунок 2, под надписью множество ЧПЭ). В работе [2] для этого пространства была предложена структура и определены правила комплексирования моделей системы связи на основе методики композиции частных показателей эффективности.

Итак, определены:

1. Множество дискрет признакового пространства

$$L = \bigcup_{i,j,k} D_{ijk}, \quad D_{ijk} = \langle W_{ijk}, J_{ijk} \rangle \tag{1}$$

каждый элемент которого – дискрета) – задается двуместным кортежем, состоящим из частной модели системы связи и значения ЧПЭ, рассчитываемого по этой модели, вместе определяющих интерпретацию системы связи.

2. Модель ситуации

$$z = \langle D, \tau \rangle, D \subset L, \tau = \tau(L) \tag{2}$$

где D – подмножество дискрет признакового пространства, τ – алгедоническая [3] характеристика гомеостатической системы

3. Множество классов ситуаций

$$K = \{A, B, C, H\} \tag{3}$$

задано аналитически и определено свойствами множества L [2].

4. Множество типов ситуаций

$$T = T_B \cup T_C, \quad T_B = \bigcup_m B_m, \quad T_C = \bigcup_n C_n \tag{4}$$

классы H и A тривиальны и не имеют типов (рисунок 2), характеризуемых различным разбиением множества дискрет на непересекающиеся подмножества (различные композиции ЧПЭ).

Задача: построить процедуры, реализующие алгоритм классификации, который в соответствии с алгедоническими свойствами множества L определит наилучшую композицию ЧПЭ и на основе анализа взаимосвязей ЧПЭ определит класс ситуации.

Основные решения. Алгоритм классификации ситуаций приведен на рисунке 1, ключевые процедуры алгоритма – типизации и экстраполяции выделены на рисунке красными прямоугольниками и обозначены соответственно буквами Т и Э. Такая структура алгоритма позволяет его отнести к ситуационным процедурам [4].

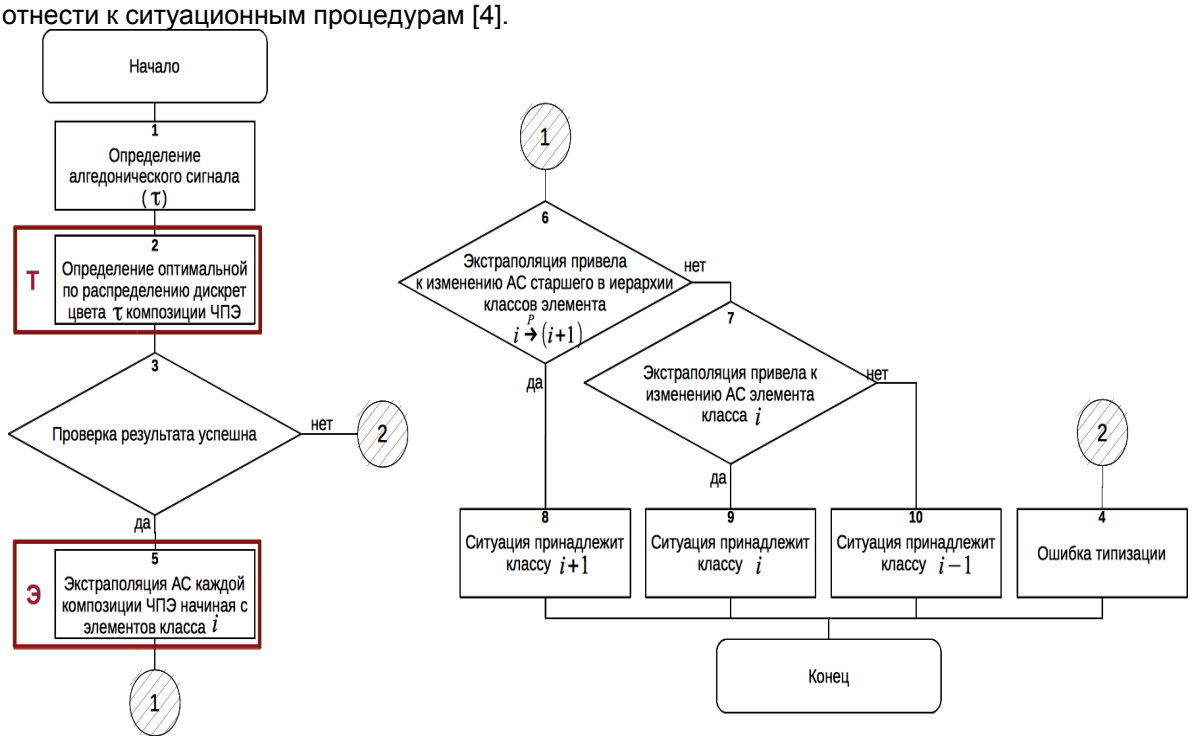


Рис. 1. Алгоритм классификации ситуаций.

Содержание этапов алгоритма отображено на диаграмме нар 2.

Анализ различных реализаций алгоритма показал, что наибольшее влияние на результаты работу алгоритма оказывает типизация ситуаций.

Основные результаты. Анализ подходов к построению процедур типизации в целом показал их соответствие подходам, применяемым при решении задачи классификации. В связи с этим, были выделены две большие группы, соответствующие метрическому и экспертному подходу к типизации. Блок-схемы алгоритмов соответствующих процедур представлены на рисунке 3.

Общей чертой обеих процедур является формирование последовательности наборов дискрет, соответствующих ситуациям класса С, упорядоченным по количеству дискрет цвета т. При этом ставится задача выбора единственной плоскости из последовательности, отвечающей решающему правилу (обладающей максимальной метрикой для случая метрической типизации или отвечающей эвристическому правилу в случае экспертной типизаций).

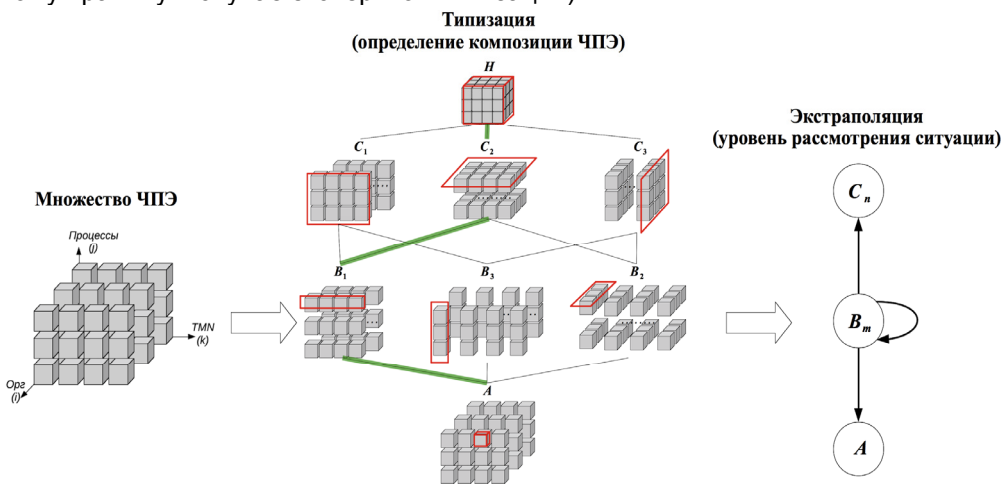


Рис. 2. Содержание этапов работы алгоритма классификации ситуаций

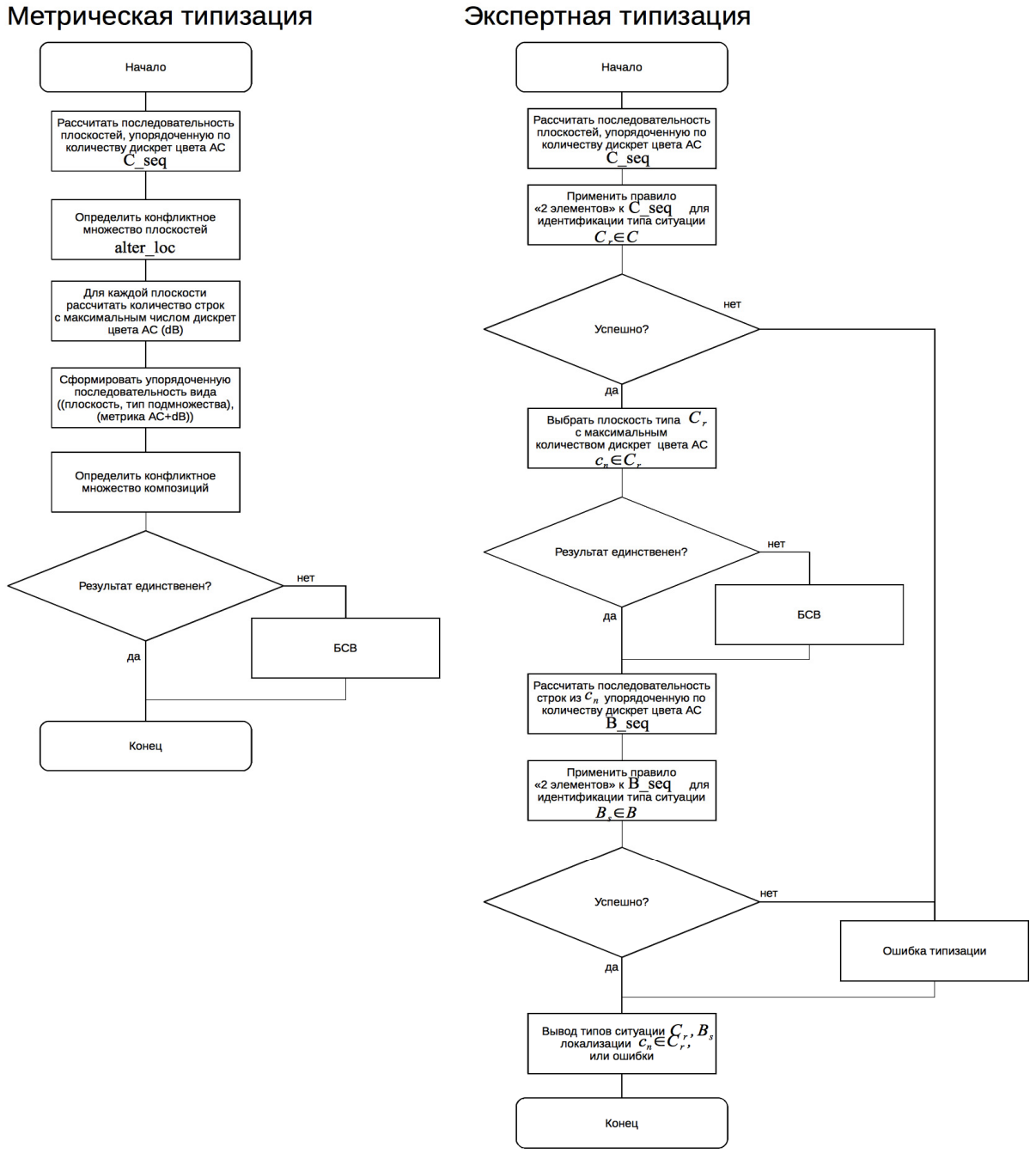


Рис. 3. Блок-схемы процедур метрической и экспертной типизации

Основное отличие двух процедур заключается в том, что экспертная типизация предполагает последовательную фиксацию классов (сначала С, потом В), а метрическая упорядочивает непосредственно композиции ЧПЭ для всех плоскостей с критическим значением метрики.

Данные прогона алгоритма классификации ситуаций для случая метрической и экспертной типизации на одинаковом объеме данных приведены в Таблице 1.

Таблица 1

Результаты прогона процедур типизации

Процедура типизации	Количество ошибок			Количество успешных попыток			Качество локализации		
	кл. «С»	кл. «В»	всего	> 1пл-ти	1 пл-ть	всего	хор	уд.	не уд.
Метрическая	0	0	0	442	558	1000	558	416	26
Экспертная	42	92	134	407	459	866	719	146	1

При этом совпадений ситуаций класса С зафиксировано в 22% случаев успешных прогонов, ситуаций класса В – в 38%.

Заключение. Согласно полученных результатов, целесообразно применить комбинацию процедур экспертной и метрической типизации в следующем порядке: сперва экспертная типизация, затем, при возникновении ошибки типизации или неудовлетворительной локализации – метрическая. Подобный подход гарантирует успешную процедуру типизации при непустом множестве ЧПЭ, характерную для метрической типизации, сохранив при этом качество экспертной типизации.

Дальнейшее совершенствование предложенных процедур лежит, по-видимому, на пути усложнения решающих правил, в частности, применения метрик, основанных на более глубоком анализе конфликтных множеств – путем решения задачи диагностики, что, однако, выходит за рамки рассматриваемого признакового пространства.

СПИСОК ЛИТЕРАТУРЫ

1. Дадаев, В.И. Открытая базовая иерархическая модель телекоммуникационной системы/В.И. Дадаев, М.В. Фёдоров, С.О. Бурлаков//Информационные технологии моделирования и управления. – 2005. – №3. – С. 422-427
2. Ковалев, И.Г. Метод композиции частных показателей эффективности в задаче типизации ситуаций в управлении телекоммуникационными системами/И.Г. Ковалев//Информационные технологии в инновациях, медико-биологических и технических науках: сборник научных трудов пятого международного научного конгресса “Нейробиотелеком-2012”. – СПб.: Политехника, 2012. – С. 45-50
3. Бир, С. Мозг фирмы: Пер. с англ./С. Бир. – М.: Радио и связь, 1993. – 416 с.
4. Поспелов, Д.А. Ситуационное управление: теория и практика/Д.А. Поспелов. – М.: Наука, 1986. – 288 с.

УДК 004.946

ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ В ИТ ИНФРАСТРУКТУРЕ ВУЗА И УГРОЗЫ БЕЗОПАСНОСТИ

Кононов Олег Александрович, Кононова Ольга Васильевна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д. 67,
e-mail: o2kon@mail.ru

Аннотация. В статье рассмотрены особенности использования технологии виртуализации в ИТ инфраструктуре ВУЗа с учетом угроз безопасности.

Ключевые слова: *технологии виртуализации, ИТ инфраструктура, угрозы безопасности.*

VIRTUALIZATION TECHNOLOGIES IN THE IT INFRASTRUCTURE OF THE UNIVERSITY AND THE SECURITY THREATS

Oleg Kononov, Olga Kononova,
Saint-Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya street 67,
e-mail: o2kon@mail.ru

Abstract. This article describes specific virtualization technology in university IT infrastructure taking into account security threats.

Keywords: *virtualization technologies, IT infrastructure, security threats.*

Введение. Технологии виртуализации в современных ИТ-инфраструктурах используются для решения следующего ряда задач [1]: виртуализация серверов; виртуализация сетей; разработка и тестирование ПО; виртуализация рабочих станций; виртуализация рабочих мест; консолидация серверов; хостинг приложений; использование унаследованного ПО; Web-хостинг. По данным Forrester, в США уже 85% представителей корпоративного сектора пользуются средствами виртуализации.

На рисунке 1 даны ожидания от внедрения технологий виртуализации [1].

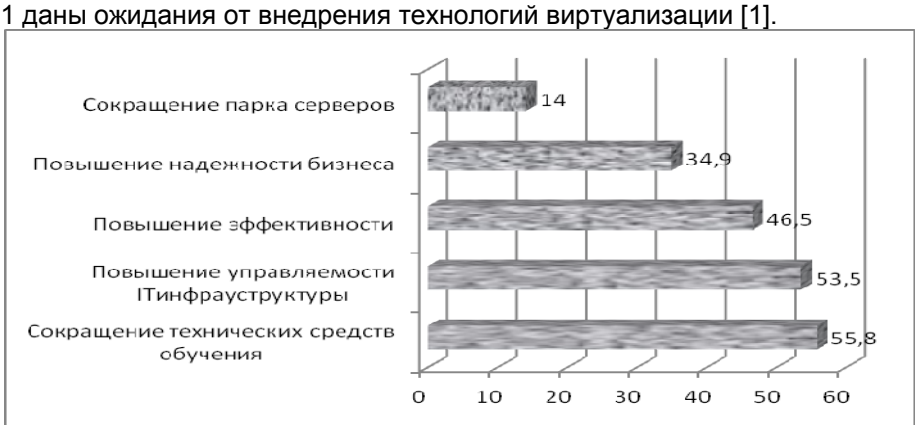


Рис. 1 Ожидания от внедрения технологий виртуализации в %

Размер рынка виртуализации аналитики оценивают по-разному, но в одном они сходятся: до 2015 года мировой рынок виртуализации будет расти. Только в России в 2015 году рынок виртуализации может достичь 500 млн. долларов по прогнозу Forrester. При этом если в расчет включить затраты на приобретение аппаратуры и сервисные услуги по внедрению виртуализации, то размер рынка публичных облаков в России, по оценке IBS, будет в три раза больше. Доля публичных облаков в мире в 2013 году составляла 40% и ожидается ее рост к концу 2015 года почти в полтора раза, отмечают аналитики Forrester. При этом средняя «плотность» виртуальных машин (ВМ) приближается к семи ВМ на сервер [1].

Внедряя в образовательный процесс технологии виртуализации, мы одновременно решаем две задачи: знакомим обучающихся с перспективными технологиями и получаем экономические, организационные и социальные преимущества от их ежедневного использования [2].

Защита среды виртуализации информационных систем компании требует эффективных решений для борьбы как с некоторыми старыми, так и с новыми, ранее неизвестными угрозами. Среди угроз виртуализации, которым открыты данные технологии, можно отметить:

– угроза компрометации гипервизора как нового, по сравнению с физической средой, элемента управления инфраструктурой;

– угроза утечки данных вследствие злонамеренных или непреднамеренных действий системного администратора, получающего доступ к данным и к инфраструктуре;

– клонирование/копирование, миграция, репликация, создание снимков виртуальных машин;

– компрометация консолидированного хранилища данных при консолидации нескольких серверов на одном аппаратном комплексе, если компания прибегает к серверной виртуализации;

– угроза несанкционированного доступа (НСД) администратора виртуальной инфраструктуры к настройкам и правам пользователей на сервере виртуализации;

– отсутствие контроля за всеми событиями информационной безопасности и невозможность расследования инцидентов при их возникновении.

Рассмотрим риски безопасности на примере наиболее распространенных технологий виртуализации в ИТ-инфраструктурах ВУЗов.

Виртуализация ресурсов и безопасность. Виртуализация ресурсов имеет расплывчатый смысл и представляет собой массу различных подходов, направленных на повышение удобства обращения пользователей с системами в целом. Применительно к реализации учебного процесса виртуализацию ресурсов наиболее эффективно применять путем размещения нескольких виртуальных серверов административной сети и сетей компьютерных классов на одном физическом сервере, например: брандмауэра, web – сервера, сервера приложений и сервера базы данных, что ведет к существенной экономии средств и представляется особенно важным в условиях дефицита средств на развитие и поддержание ИТ-инфраструктуры. Кроме того, виртуализация сервера может привести к лучшей обработке инцидентов, так как сервера можно вернуть к предыдущему состоянию с той целью, чтобы проанализировать, что происходило до и во время атаки. Данный тип виртуализации может быть использован в образовательных учреждениях любого уровня [3].

Как для ИТ персонала, так и для учебного процесса очень красивым решением является распространение возможностей виртуализации на сеть и систему безопасности. Создание и инициализация логических сетей, а также управление ими выполняется программным способом с использованием базовой физической сети в качестве удобной коммутационной панели переадресации пакетов. Как и при виртуализации серверов, из любой комбинации логических сетевых устройств и политик безопасности можно получить любую топологию. Службы сети и безопасности связаны с каждой виртуальной машиной и перемещаются вместе с ней, поэтому рабочие нагрузки можно динамически добавлять или перемещать без участия оператора.

В качестве примера использования такого подхода могут служить системы: системы HNV от Microsoft и NSX от VMware, виртуальные сетевые адаптеры (vNIC) и виртуальные коммутаторы (vSwitch) для Linux и другие. Основными целями виртуализации сетей являются: разделение и управление потоками информации, сетевая изоляция, сегментирование сети, а также защита информации при ее передаче по сети.

Виртуализация платформ и безопасность. Под виртуализацией платформ понимают создание программных систем на основе существующих аппаратно-программных комплексов (ПК или серверов), зависящих или независящих от них. Система, представляющая свои аппаратные ресурсы и программное обеспечение для реализации целевых систем, называется базовой (host), а симулируемые ею системы – гостевыми (guest). Чтобы гостевые системы могли стабильно функционировать на платформе базовой системы, необходимо, чтобы программное и аппаратное обеспечение базы было достаточно надежным и предоставляло необходимый набор интерфейсов для доступа к его ресурсам.

Наиболее интересным вариантом виртуализации платформ представляется использование так называемых виртуальных машин, которые могут оказать значительную помощь в реализации учебного процесса в физико-математических школах, а также в вузах по специальностям, связанным с подготовкой ИТ-специалистов, в условиях динамично развивающихся в последнее время

программного обеспечения, компьютерных сетей и мультимедиа технологий. ВМ позволяют запускать на одном компьютере одновременно несколько разных операционных систем (ОС) и переключаться из одной ОС в другую без перезапуска компьютера с точной эмуляцией работы полноценного компьютера.

При этом мы можем иметь несколько изолированных, т.е. защищенных друг от друга операционных систем на одной физической машине [4]. Эти системы могут быть объединены и представлять собой гомогенную или гетерогенную сеть машин, что очень важно при изучении сетевых технологий. Сейчас такой подход широко используется не только в компьютерных классах, но и на личных ПК студентов и преподавателей при изучении ИТ-дисциплин.

Высокая степень защищенности базовой машины от приложений виртуальных машин позволяет безопасно организовать учебный процесс при обучении программированию для отладки и тестирования создаваемых программ без каких-либо ограничений для пользователя.

Виртуализация платформ на основе серверов позволяет запустить ОС пользователя (Linux, Windows 7 и т.д.) внутри виртуальной машины на сервере и работать с ней удаленно с любого устройства (Citrix XenDesktop, VMware View, Microsoft VDI, Quest vWorkspace). А это значительно расширяет возможности, как студентов, так и преподавателей в части дистанционного взаимодействия с информационными системами вуза. При этом применение в компьютерных классах для реализации интерфейса пользователя тонких или нулевых клиентов вместо ПК существенно снижает совокупную стоимость владения ИТ инфраструктурой вуза [5]. Изоляция процессов и данных виртуальных машин позволяет на одном физическом устройстве (сервере, рабочей станции) обрабатывать общедоступную и конфиденциальную информацию. Тем не менее гарантия изоляции виртуальных машин по данным не может быть стопроцентной, так как связана с потенциальными уязвимостями гипервизора.

Виртуализация приложений и безопасность. Виртуализация уровня приложений не похожа на все остальные виды виртуализации: если в предыдущих случаях создаются виртуальные среды или виртуальные машины, использующиеся для изоляции приложений, то в данном случае само приложение помещается в контейнер с необходимыми элементами для своей работы: файлами реестра, конфигурационными файлами, пользовательскими и системными объектами. В результате получается приложение, не требующее установки на аналогичной платформе. При переносе такого приложения на другую машину и его запуске, виртуальное окружение, созданное для программы, разрешает конфликты между ней и операционной системой, а также другими приложениями. В качестве примера систем, обеспечивающих виртуализацию приложений, можно выделить: ThinApp, App-V, XenApp. Большим подспорьем такой подход служит для системных администраторов в части защиты операционной системы от приложений и обеспечения независимости приложений от реальных компонентов (например, динамических библиотек DLL) [6]. Виртуализация приложений позволяет запускать приложения локально и экономить ресурсы сервера, устраняет единые точки отказа и снимает ограничения на работу в сети. Однако технология виртуализации приложений не приводит к повышению уровня информационной безопасности, так как виртуализированные приложения не имеют гарантированной взаимной изоляции по миграции программного кода.

По сравнению с физическими машинами и количеству критических уязвимостей в ОС (Windows, Linux), число уязвимостей в платформах виртуализации ничтожно мало. При тестировании продукции VMware (гипервизор и сопутствующем ПО) было выявлено около 15 критических уязвимостей, связанных с безопасностью. В любом случае, возможность использования злоумышленниками конкретных уязвимостей может быть ограничена с помощью программно-технических или организационных мер. Безопасно построенные виртуализированные и облачные среды с использованием требований таких стандартов, как NIST, PCI–DSS, VMware Security Hardening Best Practice, CIS, DISA, СТО БР ИББС, ФЗ–152 (РД ФСТЭК), не уступают по уровню надежности и защищенности традиционной физической системе, а в чем-то даже превосходят ее [8].

Заключение. Угрозами безопасности для виртуальных инфраструктур являются атака на гипервизор с виртуальной машины; атака на гипервизор из физической сети; атака на диск виртуальной машины; атака на средства администрирования виртуальной инфраструктуры; атака на виртуальную машину с другой виртуальной машины; атака на сеть репликации виртуальных машин; неконтролируемый рост числа виртуальных машин. Проблемы внедрения технологий виртуализации связаны с тем, что с одной стороны, традиционные средства защиты информации не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. С другой стороны, они не защищают от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры. Современные средства виртуализации гарантируют надежность работы виртуальных машин, перераспределяя угрозы, сужая область действия каждой из них и локализуя последствия. Однако, за это перераспределение приходится «платить» возникновением принципиально новых угроз, обусловленных спецификой организации и эксплуатации виртуальных ресурсов. Решение лежит в одновременном применении защитных механизмов, встроенных в средства виртуализации, специализированных инструментов защиты, а также тех инструментов защиты, которые уже используются в ИТ подразделениях ВУЗов.

СПИСОК ЛИТЕРАТУРЫ

1. Обойдемся без железа. Российская Бизнес-газета № 944 от 22 апреля 2014 г.
2. Кононов О.А., Кононова О.В. Виртуальные машины как инструмент организации учебного процесса в области информационных технологий // XI Санкт-Петербургская международная конференция «Региональная информатика – 2008 (РИ–2008)»: материалы конференции. – СПб.: СПОИСУ, 2008. С. 203–204.
3. Кононов О.А., Кононова О.В. Технологии виртуализации и подготовка ИТ-специалистов // Интеллектуальные технологии в экономике и управлении: Сборник научных трудов. – СПб.: Изд-во СПбГУЭФ, 2009. С.118–123.
4. Кононов О.А., Кононова О.В. Технология виртуализации как инструмент подготовки ИТ-специалистов // XI Санкт-Петербургская международная конференция «Региональная информатика – 2008 (РИ–2008)»: труды конференции. – СПб.: СПОИСУ, 2009. С. 253–256.
5. Кононов О.А., Кононова О.В. Технология виртуализации как инструмент подготовки по направлению «Бизнес-информатика» // Экономика. Налоги. Право. Журнал ФГОУ ВПО «Всероссийская гос. налоговая академия Мин. финансов РФ», № 6, 2010.С.102–106.
6. Кононов О.А. Технология виртуализации как инструмент совершенствования ИТ-структуры учебных заведений // Информационные технологии для Новой школы. Материалы международной конференции. Т.2. СПб.: ГБОУ ДПО ЦПКС «Региональный центр оценки качества образования и информационных технологий», 2012. С. 106–109.
7. Писарев А.И. Виртуализация и безопасность: риска нет? // Электронный ресурс: http://www.cnews.ru/reviews/free/security2012/articles/ article17.shtml

УДК 51.007.004

ОЦЕНИВАНИЕ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ

Копыльцов Антон Александрович,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина),
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mail: kopyl2001@mail.ru

Аннотация: В статье рассмотрены проблемы обработки слабо формализованной информации. Особое внимание уделено оцениванию безопасности поступающей информации. Предложен алгоритм обработки слабо формализованной информации и приведено его обоснование. В основе алгоритма лежат принципы обработки слабо формализованной информации в живых системах.

Ключевые слова: *слабо формализованная информация; обработка информации.*

SAFETY EVALUATION ENTERS WEAKLY FORMALIZED INFORMATION

Anton Kopyltsov,
The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str. 5,
e-mail: kopyl2001@mail.ru

Abstract: The article deals with the problem of weakly formalized information handling. Particular attention is paid to the safety evaluation of incoming information. An algorithm for treating weakly formalized information and justification is given. The algorithm based on the principles of treatment of weakly formalized information in living systems.

Keywords: *weakly formalized information; data processing.*

Введение. В последние годы много внимания уделяется обработке слабо формализованной информации, одним из важных показателей которой, является безопасность этой информации и методы ее оценивания [4], [14]. 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 достоверноси поступающей слабо формализованной информации» решает задачу по аналогии с живой природтой, 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.) [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. Для обработки слабо формализованной информации могут быть использованы распределенные информационно-вычислительные системы или кластеры высокопроизводительных параллельных вычислений.

Этапы обобщенного алгоритма. Последовательность обработки информации в обобщенном алгоритме содержит следующие этапы (Рисунок 1):

1. В модуле «Сбор информации» собирается информация, которая поступает от технической системы, с помощью различных датчиков.
2. В модуль «Распознавание информации» поступает информация из модуля «Сбор информации». В этом модуле происходит разделение информации на аудио, видео, тактильную и другие виды информации. Часто наблюдаемый объект проявляет себя в нескольких видах информации, например, в аудио и видео.
3. В модуль «Классификация информации» информация поступает из модуля «Распознавание информации». Там она разделяется на классы $K_1,...,K_i,...,Kn,$ где n – число классов (величина n зависит от конкретной задачи). Классы содержат один из видов информации (зрение, слух, осязание, вкус и обоняние) или комбинации из них по два, по три и более. Число различных видов информации может быть изменено, т.е. увеличено или уменьшено в зависимости от конкретной задачи.
4. В модулях «Свертка информации» осуществляется обработка информации по определенному алгоритму свертки. После обработки получаем новую информацию для каждого из n классов.
5. В модулях «Оценивание достоверности информации» осуществляется оценивание достоверности информации, полученной после свертки, в каждом из n классов. Это достигается методом сравнения вновь поступившей информации с ранее поступившей информацией, которая хранится в модуле «Хранилище». Если достоверность поступившей информации меньше некоторого значения, заранее выбранного для каждого класса, то считается, что информация не достоверная и происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму и информация попадает в другой класс.
6. Оценивание безопасности информации происходит в n модулях «Оценивание безопасности информации» для каждого класса, методом ее сравнения с ранее поступившей информацией. Если уровень опасности поступившей информации превышает некоторое заранее взятое для каждого из n классов значение, то поступившая информация считается опасной и происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму и информация попадает в другой класс.
7. В модулях «Установление связей» осуществляется установление связей в каждом из n классов между вновь поступившей информацией ранее поступившей. В случае, когда число связей не превышает некоторой, заранее заданной для каждого из n классов величины, происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму и информация попадает в другой класс.
8. В модулях «Оценивание вероятности» происходит оценивание в каждом из n классов вероятности, с которой можно доверять недавно полученной информации. Это достигается с помощью вероятностного алгоритма для оценивания работоспособности системы наблюдения.
9. В модулях «Поддержка принятия решений» происходит поддержка принятия решений в n классах.

10. В модуле «Обобщенная поддержка принятия решений» происходит сборка сгенерированных решений из всех n классов и на их основе формируется новая обобщенная совокупность решений.

11. Сравнение принятого решения с решениями, которые были приняты ранее, происходит в модуле «Определение числа связей». Это достигается путем сравнения с ранее поступившей информацией, хранящейся в модуле «Хранилище». В случае, когда число подтверждений не превосходит некоторого, заранее выбранного числа, то, происходит переход в модуль «Распознавание информации, где происходит повторная обработка информации согласно алгоритму и информация попадает в другой класс.

12. Выработка устойчивой реакции на неоднократно поступающую информацию и ее запоминание происходит в модуле «Выработка устойчивой реакции». Это достигается методом сравнения вновь поступившей информации и информации полученной ранее.

13. Генерация решений происходит в модуле «Генерация решений».

14. Поступившая ранее информация собирается в модуле «Хранилище». В этом модуле генерируется новая информация с учетом сведений о вновь поступившей информации и ранее записанной информацией. Там же проводится проверка информации на степень ее новизны. В случае, когда информация действительно является новой, то эта информация поступает в модуль «Сбор информации» для последующей обработки согласно алгоритму.

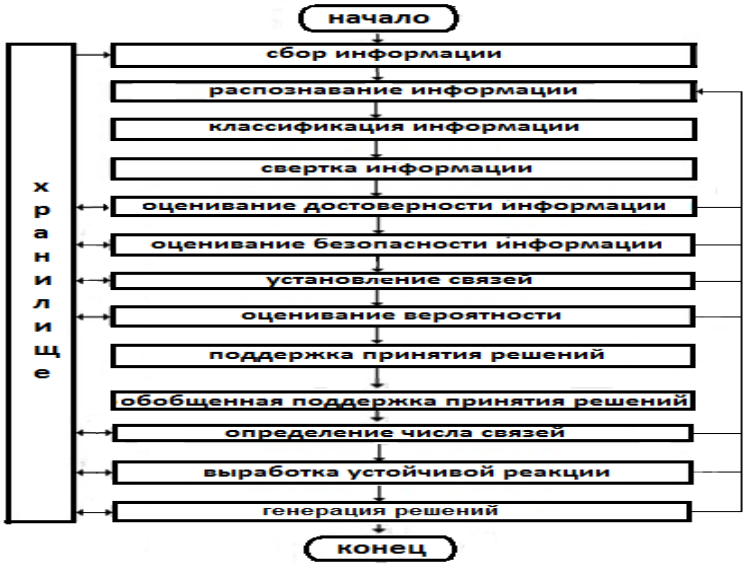


Рис. 1. Блок-схема обобщенного алгоритма.

Обоснование обобщенного алгоритма. За основу взяты способы хранения и обработки информации в живых организмах, которые были открыты и изучены в XIX-XXI веках [1], [2], [22], [23].

Известно, что в живых организмах происходит сбор, распознавание и классификация информации. Информация собирается с помощью различных органов чувств (зрение, слух, обоняние, осязание, вкус и др.). На 1 этапе в обобщенном алгоритме информация собирается в модуле «Сбор информации».

Распознавание и классификация информации осуществляется в мозге. В процессе эволюции распознавание информации (например, враг или друг, пища или яд и др.) достигло большого совершенства и специализации. Например, орлы отличаются острым зрением, собаки и мыши – острым обонянием, совы – острым слухом, летучие мыши – очень чувствительны к ультразвуку, змеи очень чувствительны к изменению температуры и т.д. Человек обладает пятью основными органами чувств (зрением, слухом, обонянием, осязанием, вкусом). На втором этапе распознавание информации осуществляется в модуле «Распознавание информации», в котором происходит разделение информации на аудио, видео, тактильную и другие виды информации и их сочетания по два, по три и т.д.

В живых организмах происходит классификация информации в зависимости от их образа жизни. Есть организмы, которые обладают зрением и слухом (например, птицы), слухом, ультразвуком, но плохим зрением (например, летучие мыши). Классификация информации осуществляется на 3 этапе обобщенного алгоритма на классы $K_1,...,K_i,...,Kn$, где n – число классов (величина n зависит от конкретной задачи). Классы содержат один из видов информации (зрение, слух, осязание, вкус и обоняние) или комбинации из них по два, по три и более.

Информация об объекте, который наблюдается в различных диапазонах одновременно, обрабатывается и хранится после обработки не в разных структурах мозга (как считалось раньше), а

в одной и той же (некоторой группе нейронов размещенных довольно компактно). Известно, что нейроны, ответственные за хранение и обработку информации в различных диапазонах, размещены в коре головного мозга неравномерно. Например, в затылочной части мозга наибольшую концентрацию имеют нейроны ответственные за зрение (зрительная зона коры головного мозга), но это не означает, что там отсутствуют нейроны ответственные за хранение и обработку другой информации. Причем, с течением времени количество задействованных нейронов возрастает и, в случае появления новой информации и ее накопления, количество связей между нейронами так же увеличивается. Причем обработка разнообразной информации, хранящейся в некоторой группе нейронов, осуществляется по аналогичному алгоритму. Это реализовано на четвёртом этапе обобщенного алгоритма с помощью алгоритма свертки. После применения алгоритма свертки получаем новую информацию (свертку) для каждого из n классов.

В живом организме при поступлении информации извне происходит оценивание достоверности и безопасности информации, путем сравнения с ранее поступившей информацией [2]. Для эволюции оценивание достоверности и безопасности поступающей извне информации очень важно, т.к. если по каким-либо причинам живой организм это не делает или делает плохо, например, травма головы, или проблемы с памятью, то он погибает [2]. Это реализовано на 5-м и 6-м этапах обобщенного алгоритма в модулях «Оценивание достоверности информации» и «Оценивание безопасности информации», путем сравнения вновь поступившей информации с ранее поступившей информацией. Если достоверность поступившей информации меньше некоторого заранее выбранного значения для каждого класса, то считается, что информация не достоверная и происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму. Если уровень опасности поступившей информации превышает некоторое заранее взятое для каждого из n классов значение, то поступившая информация считается опасной и происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму.

В мозге новые знания генерируются путем сравнения вновь поступившей и обработанной специальным образом информацией с ранее поступившей и также обработанной определенным образом информацией. Считается, что у человека развито ассоциативное мышление, т.е. вновь поступившая информация запоминается и обрабатывается эффективно, если возникают какие-либо ассоциации, т.е. если эта вновь поступающая информация может быть каким-то образом связана с ранее поступившей информацией и хранящейся в мозге. То есть, вновь поступившая информация в первую очередь сравнивается с информацией в мозге, уже прошедшей некоторую обработку [2]. Это реализовано на 7-м этапе обобщенного алгоритма в модулях «Установление связей» путем установление связей в каждом из n классов между вновь поступившей информацией и ранее поступившей информацией. В случае, когда число связей не превышает некоторой, заранее заданной для каждого из n классов величины, происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму.

На 8-м этапе в модулях «Оценивание вероятности» происходит оценивание в каждом из n классов вероятности, с которой можно доверять недавно полученной информации. Это достигается с помощью вероятностного алгоритма. В случае, когда вероятность не превосходит некоторой, заранее заданной величины, определяемой для каждого из n классов, то происходит переход в модуль «Распознавание информации», где проводится повторная обработка информации согласно алгоритму.

Живые организмы принимают решения после получения какой-либо информации. Если это пища, то нападают, а если хищник, то затаиваются или убегают. Живой организм может принять решение по одному классу (например, при выстреле ружья почти все животные убегают, если раньше им приходилось сталкиваться с охотником с ружьем (один класс – аудио)). Если же животному не приходилось встречаться с охотником, то оно может с ним встретиться (класс – видео). В случае повторного выстрела получим классы: аудио, видео, аудио-видео, а если охотник попадет, то возможно получим еще и классы: аудио-видео-тактильный, аудио-тактильный, видио-тактильный, например. Это реализовано на этапах 9 и 10 обобщенного алгоритма в модулях «Поддержка принятия решений», в которых осуществляется поддержка принятия решений в n классах. Совокупность сгенерированных решений зависит от конкретной задачи. На этапе 10 в модуле «Обобщенная поддержка принятия решений» происходит сборка сгенерированных решений из всех n классов и на их основе формируется новая обобщенная совокупность решений.

Основная функция мозга, обеспечивающая выживание организма в окружающей среде, т.е. в мозге учитываются приоритеты при обработке информации. Например, если животное почувствовало опасность, то он замирает и прислушивается, готовое в любой момент, либо напасть, либо убежать, на основании предыдущего жизненного опыта. Это реализовано на этапе 11 обобщенного алгоритма в модуле «Определение числа связей» путем сравнение принятого решения с решениями, которые были приняты ранее. В случае, когда число подтверждений не превосходит некоторого, заранее

выбранного числа, то, происходит переход в модуль «Распознавание информации, где происходит повторная обработка информации согласно алгоритму.

Наблюдательность – важное свойство эволюции, позволяющее замечать повторяющиеся факты и явления, т.е. выявлять периодические временные ряды, закономерности в событиях и явлениях. Если какое-либо событие у живого организма уже было один или несколько раз, то вырабатывается стереотип поведения (условный рефлекс по И.П. Павлову). Это реализовано на этапе 12 обобщенного алгоритма в модуле «Выработка устойчивой реакции». Это достигается методом сравнения вновь поступившей информации и информации полученной ранее.

Живой организм на основе информации поступившей через глаза, уши, нос и другие органы чувств принимает окончательное решение, например, нападать, затаиться или убегать. Если животное, например, осталось в живых, то эта информация (о поведении в такой ситуации) сохраняется в памяти. В случае повторения подобных ситуаций вырабатывается стереотип поведения (условный рефлекс), что обеспечивает выживание организма [1], [2], [22], [23]. Это реализовано на этапах 13 и 14 обобщенного алгоритма в модуле «Генерация решений». Поступившая ранее информация обрабатывается и собирается в модуле «Хранилище», генерируется новая информация с учетом сведений о вновь поступившей информации и ранее записанной информации, осуществляется проверка информации на степень ее новизны. В случае, когда информация действительно является новой, она поступает в модуль «Сбор информации» для последующей обработки согласно алгоритму.

Заключение. Предложен обобщенный алгоритм обработки слабо формализованной информации, включает 14 этапов. Функциональные возможности обобщенного алгоритма обработки слабо формализованной информации следующие: оценивание достоверности получаемой информации; оценивание безопасности получаемой информации; оценивание вероятности, с которой можно доверять получаемой информации; выработка устойчивой реакции на получаемую информацию и ее запоминание; поддержка принятия решений; генерация новой информации. Приведено обоснование предложенного алгоритма на основе принципов обработки слабо формализованной информации в живых системах.

СПИСОК ЛИТЕРАТУРЫ

1. Бабский Е.Б.. Физиология человека и животных. – М: Высшая школа, 1990, 580 с.
2. Кандел Э. В поисках памяти, - М: Династия, 2012, 610 с.
3. Копыльцов А.А. Сохранение конфиденциальности данных при поддержке принятия решений, на основе извлекаемой специальным образом информации // Материалы VIII Санкт- Петербургской межрегиональной конференции «Информационная безопасность регионов России» (23 – 25 октября 2013 г.). Санкт-Петербург: СПОИСУ. – 2013, С.104.
4. Копыльцов А.А., Копыльцов А.В. Обработка слабо формализованной информации, поступающей от технических систем // Вестник Нижневартовского государственного гуманитарного университета. – 2013. - № 1, С. 32–36.
5. Копыльцов А.А., Копыльцов А.В. Цифровой образовательный ресурс «Краткая история моделирования» и его применение в учебном процессе // Материалы сетевой международной научно-практической конференции «Электронное обучение в ВУЗе и школе» (16-19 апреля 2014 г.). СПб: РГПУ. – 2014. – С. 153–155.
6. Копыльцов А.А. Алгоритм коррекции связей между фрагментами слабо формализованной информации и генерация новой информации // Вестник Нижневартовского государственного университета. – 2014, № 3. - С. 28–34.
7. Копыльцов А.А. Обработка слабо формализованной информации в живых и технических системах // Материалы Всероссийской научно-практической конференции студентов, магистров, аспирантов «Современное программирование» (16–17 апреля 2014 г.). Нижневартовск: Издательство Нижневартовского государственного университета. – 2014, С. 117–121.
8. Копыльцов А.А. Обработка слабо формализованной информации при недостатке информации // Материалы XIII Санкт-Петербургской международной конференции «Региональная информатика – 2012» (24–26 октября 2012 г.). Санкт-Петербург: СПОИСУ. – 2012, С. 374.
9. Копыльцов А.А. Особенности обработки слабо формализованной информации // Материалы XIV Санкт-Петербургской международной конференции «Региональная информатика – 2014» (29 – 31 октября 2014 г.). Санкт-Петербург: СПОИСУ. – 2014, С. 555–556.
10. Копыльцов А.А. Применение обобщенного алгоритма обработки слабо формализованной информации для управления неравновесной химической реакцией // Инженерный вестник Дона. 2015. № 1. ч.2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2812
11. Копыльцов А.А. Программа для обработки слабо формализованной информации, поступающей от технических систем // Свидетельство о государственной регистрации программы для ЭВМ № 2013617310. Правообладатель: ФГБОУ ВПО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им В.И. Ульянова (Ленина)» (СПбГЭТУ). Заявка № 2013615041. Дата поступления 19 июня 2013 г. Дата государственной регистрации в Реестре программ для ЭВМ 08 августа 2013 г.
12. Копыльцов А.А. Слабо формализованная информация и алгоритмы ее обработки // Материалы XIV Санкт-Петербургской международной конференции «Региональная информатика – 2014» (29–31 октября 2014 г.). Санкт-Петербург: СПОИСУ. – 2014. – С. 556–557.
13. Копыльцов А.А. Цифровой образовательный ресурс «Обработка слабо формализованной информации в живых и технических системах» // Материалы сетевой международной научно-практической конференции «Электронное обучение в ВУЗе и школе» (16-19 апреля 2014 г.). СПб: РГПУ. – 2014. – С. 151–153.
14. Копыльцов А.А., Копыльцов А.В. Алгоритм обработки слабо формализованной информации, поступающей от технических систем // Известия СПбГЭТУ «ЛЭТИ» (известия государственного электротехнического университета), серия «Информатика, управление и компьютерные технологии». – 2012. – № 8, С. 30–36.
15. Копыльцов А.А., Копыльцов А.В. Качественная и количественная слабо формализованная информация и ее обработка // Материалы XIV Санкт-Петербургской международной конференции «Региональная информатика – 2014» (29–31 октября 2014 г.). Санкт-Петербург: СПОИСУ. – 2014, С. 557.
16. Копыльцов А.А., Копыльцов А.В. Обобщенный алгоритм обработки слабо формализованной информации и его применение // Вестник Нижневартовского государственного университета. – 2014. – № 35, С. 35–44.

17. Копыльцов А.А., Копыльцов А.В. Технические системы и слабо формализованная информация // Материалы XIII Санкт-Петербургской международной конференции «Региональная информатика – 2012» (24–26 октября 2012 г.). Санкт-Петербург: СПОИСУ. – 2012, С. 375.
18. Копыльцов А.А., Нечитайленко Р.А. Кластерное атрибутирование объектов информационной обработки по понятийным частным и интегральным признакам // Материалы XII Санкт-Петербургской международной конференции «Региональная информатика – 2010» (20–22 октября 2010 г.). Санкт-Петербург: СПОИСУ. – 2010, С. 49–50.
19. Копыльцов А.А., Нечитайленко Р.А. Обеспечение пороговой безопасности обработки слабо формализованной информации при распределенном управлении с целью принятия решений // Труды VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (26–28 октября 2011 г.). Санкт-Петербург: СПОИСУ. – 2011. С, 154–155.
20. Копыльцов А.А. Модель классификации информации и алгоритм ее предварительной обработки для статических и динамических объектов // Известия СПбГЭТУ «ЛЭТИ» (известия государственного электротехнического университета), серия «Информатика, управление и компьютерные технологии». – 2013, № 6. С. 134–139.
21. Копыльцов А.А. Обработка информации в живых и технических системах // Материалы XIII Санкт-Петербургской международной конференции «Региональная информатика – 2012» (24–26 октября 2012 г.). Санкт-Петербург: СПОИСУ. – 2012, С. 373–374.
22. Павлов И.П. Избранные труды по физиологии высшей нервной деятельности. – М.: Наука, 1951, 230 с.
23. Сеченов И.М. Рефлексы головного мозга. – М: Высшая школа, 1980, 160 с.

УДК 57.054

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ЛОКАЛЬНОЙ РЕГУЛЯЦИИ КРОВОТОКА

Копыльцов Александр Васильевич,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина),
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mail: kopyl2001@mail.ru

Аннотация: В статье рассмотрены проблемы информационной безопасности при регуляции кровотока. Информация поступает от интерорецепторов и на основании этой информации осуществляется регуляция диаметра артериол. В случае кратковременного выброса продуктов метаболизма, информация с интерорецепторов о локальном повышении концентрации продуктов метаболизма может привести либо к резкому сужению артериол, либо к резкому их расширению. В обоих случаях это может привести к необратимым последствиям, либо к спазмам сосудов, либо к резкому понижению давления, что в свою очередь может привести к летальному исходу.

Ключевые слова: *регуляция; кровоток; информация; безопасность*

INFORMATION SECURITY IN LOCAL BLOOD FLOW REGULATION

Alexander Kopyltsov,
The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str. 5,
e-mail: kopyl2001@mail.ru

***Abstract*:** The article deals with the problem of information security in the regulation of blood flow. The information comes from interoceptors and on the basis of this information is the regulation of the diameter of the arterioles In the case of short-term release of metabolic products, with interoceptors information about the local increase in the concentration of metabolic products can lead either to a sharp narrowing of arterioles or a sharp expansion. In both cases, this can lead to irreversible consequences, either to vasospasm, or to a sharp decrease in pressure, which in turn can lead to death.

Keywords: *regulation; blood flow; information; security*

Введение. 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, слоя и

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 [1], [2]. 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 [3], [4]. 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 или резкому снижению давления.

Описание модели. 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 следующей системой дифференциальных уравнений [7], [8]. В эритроците:

$$\left.\begin{aligned} \frac{\partial P}{\partial t} + V\nabla P = D_{o2E}\nabla^2 P + \frac{\rho(P,SS)}{\alpha_E} \\ \frac{\partial SS}{\partial t} + V\nabla SS = D_{Hb}\nabla^2 SS + \frac{\rho(P,SS)}{[Hb]_T} \end{aligned}\right\}. \quad (1)$$

Где

$$[Hb]_T = [Hb] + [HbO_2], \quad SS = \frac{[HbO_2]}{[Hb]_T},$$

$$\rho(P,SS) = k + [HbO2] - k - [Hb][O2] = k + [Hb]T\ SS - k - [Hb]T\ (1 - SS)\ aE\ P.$$

В слое (между эритроцитом и тканью):

$$\frac{\partial P}{\partial t} + V\nabla P = D_{O2C}\nabla^2 P\ . \quad (2)$$

В ткани:

$$\left.\begin{aligned} \frac{\partial P}{\partial t} = D_{o2M}\nabla^2 P + \frac{\sigma(P,SS)}{\alpha_M} - \frac{W}{\alpha_M} \\ \frac{\partial SS}{\partial t} = D_{Mb}\nabla^2 SS + \frac{\sigma(P,SS)}{[Mb]_T} \end{aligned}\right\}, \quad (3)$$

где

$$[\mathrm{Mb}]_\mathrm{T} = [\mathrm{Mb}] + [\mathrm{MbO_2}]\ ,\ \mathrm{SS} = \frac{[\mathrm{MbO_2}]}{[\mathrm{Mb}]_\mathrm{T}}\ ,$$

$$\sigma(P,S) = k1 + [MbO2] - k1 - [Mb][O2] = k1 + [Mb]T\ S - k1 - [Mb]T\ (1 - S)\ aMP.$$

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 (интерстициальном пространстве и капиллярном эндотелии) и кровеносных сосудах описывается следующей системой дифференциальных уравнений. В ткани:

$$\frac{\partial C}{\partial t} = D_{MpM}\nabla^2 C + \beta W^n + \frac{\gamma\varepsilon}{P+\varepsilon}. \quad (4)$$

В слое (интерстициальном пространстве и эндотелии):

$$\frac{\partial C}{\partial t} = D_{MpC}\nabla^2 C \quad (5)$$

В капилляре:

$$\frac{\partial \mathrm{C}}{\partial \mathrm{t}} + \mathrm{V}\nabla\mathrm{C} = \mathrm{D}_{\mathrm{MpB}}\nabla^2\mathrm{C}, \quad (6)$$

где

P – парциальное давление кислорода,

W – скорость поглощения кислорода тканью,

V – локальный вектор скорости кровотока,

$DO2E$, $DO2E$, $DO2M$ – коэффициенты диффузии кислорода в эритроците, слое (плазме, эндотелии, интерстициальном пространстве) и ткани,

DHb, DMb – коэффициенты диффузии гемоглобина и миоглобина,

aE, aM – коэффициенты растворимости кислорода в эритроцитах и ткани,

$[HbO2]$ – концентрация оксигемоглобина,

$[Hb]$ – концентрация гемоглобина,

$[O2]$ – концентрация кислорода,

$[MbO2]$ – концентрация оксимиоглобина,

$[Mb]$ – концентрация миоглобина,

$k-$, $k+$, $k1-$, $k1+$ – константы скоростей биохимических реакций,

t – время,

C – концентрация продуктов метаболизма,

$DMpM$, $DMpC$, $DMpB$ – коэффициенты диффузии продуктов метаболизма в ткани, слое (интерстициальном пространстве и капиллярном эндотелии) и капилляре,

$\beta, \gamma, \varepsilon, n$ – коэффициенты.

Таким образом, уравнения (1)–(6) описывают транспорт кислорода и продуктов метаболизма в эритроците, плазме, капиллярном эндотелии, интерстициальном пространстве и ткани [5], [6].

Математическая модель регуляции кровотока и транспорта кислорода в ткани учитывает строение сосудистой сети, включающей артериолы $(A2, A3, A4)$, венулы $(V2, V3, V4)$, и капилляры (C) между артериолами $A4$ и венулами $V4$. Кровь протекает последовательно через артериолы $(A2, A3, A4)$, капилляры (C) и венулы $(V2, V3, V4)$. Общее число артериол и венул в ветвлениях порядков 2, 3 и 4 обозначается через $n2, n3$ и $n4$, соответственно. Число капилляров между артериолой $A4$ и венулой $V4$ обозначается $n5$. 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. Согласно [1] градиент давления

$$\nabla P = Q / G, \quad (7)$$

где Q – объемный поток плазмы и эритроцитов, G – проводимость сосуда и

$$G = \left[\frac{128\mu_B L}{\pi d^4}\right]^{-1},$$

– для артериол и венул,

$$G = \left[\frac{128\mu_B L}{\pi d^4} + \frac{128\mu_P L}{\pi d^3} \sum_j \Delta P_j \right]^{-1},$$

– для капилляров,

где μB и μP – вязкость крови и плазмы крови,

L и d – длины и диаметры сосудов,

ΔPj – безразмерный дополнительный перепад давления на j -ом эритроците.

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. Поток продуктов метаболизма из венул в артериолы (из расчета на единицу длины сосуда) равен [1]

$$F = K(Cv - Ca), \tag{8}$$

где K – проницаемость ткани для продуктов метаболизма,

Cv и Ca – концентрации продуктов метаболизма в венуле и артериоле, причем

$$\alpha = 2\pi \ln\left[\frac{1}{\sigma}\right], \quad \sigma = \frac{R_V}{2R_a}\left(c\,d - 1 - \left(\left(c^2 - 1\right)\left(d^2 - 1\right)\right)\right)^{0,5}, \; c = 1 + \frac{\delta}{R_V}, \; d = 1 + \frac{\delta + 2R_a}{R_V},$$

где d – расстояние между артериолой и венулрой,

Ra и Rv – радиусы артериолы и венулы [1], [8].

Продукт метаболизма, после поступления из венулы в артериолу, воздействует на гладкие мышцы артериолы, и радиус артериолы Ra изменяется следующим образом

$$Ra = R\max - (R\max - R\min)\, e - a\, C, \tag{9}$$

где $R\max$ и $R\min$ – максимальный и минимальный радиус артериолы,

C – концентрация продукта метаболизма в артериоле,

a – постоянная [1].

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. Полученная система дифференциальных уравнений (1)–(9) решалась при начальных условиях:

$$P = P0,\; SS = SS0,\; S = S0,\; C = C0,$$

где $P0, SS0, S0, C0$ – известные функции z и r.

В качестве граничных условий использовались условия симметричности и условия неразрывности потоков веществ на границах: эритроцит – плазма, плазма – эндотелий, эндотелий – интерстициальное пространство, интерстициальное пространство – ткань. На оси капилляра радиальная составляющая потока всех веществ отсутствует. Система уравнений решалось методом конечных разностей. Таким образом, решая систему уравнений, мы имеем распределение кислорода и продуктов метаболизма в кровеносном сосуде и окружающей ткани.

При исследовании кровотока и транспорта кислорода в ткани наибольший интерес представляют стационарные состояния организма, поскольку большую часть жизни человек находится в стационарном состоянии (во время сна, на работе, при ходьбе и т.д.). Согласно расчетам, проведенным для стационарных условий, радиусы артериол увеличиваются при увеличении потребления кислорода тканями, что соответствует экспериментальным данным [1]. Сравнение радиусов артериол при различных скоростях потребления кислорода тканями (W) показывает, что диаметр артериол меньшего сечения достигает своей максимальной величины при меньшем значении W, чем диаметр артериол большего сечения. Например, артериолы 4-ой генерации $A4$ достигают максимального радиуса при W ~ 18 мл/100 г/мин, артериолы $A3$ – при W ~ 20 мл/100 г/мин, а артериолы $A2$ при W ~ 24 мл/100 г/мин.

Это объясняется тем, что вазоактивный продукт метаболизма поступает из ткани в венозное русло и затем частично диффундирует из венул в артериолы и, следовательно, его концентрация в артериолах увеличивается с увеличением W, причем это увеличение несколько больше в малых артериолах, чем в широких артериолах, поскольку малые артериолы ближе расположены к источнику вазоактивных продуктов метаболизма.

При изменении W от минимального значения до максимального, под воздействием вазоактивных продуктов метаболизма на гладкие мышцы, оплетающие артериолы, сечение сосудов увеличивается и объемная скорость кровотока Q возрастает. Кровоток увеличивается в 1,64 раза при увеличении W от 4 до 8 мл/100 г/мин и в 2,23 раза при увеличении W от 8 до 16 мл/100 г/мин. Согласно экспериментальным данным при аналогичных изменениях W величина Q увеличивается в 1,6–1,8 и 2,5–2,7 раза соответственно [1].

Таким образом, модель дает разумную аппроксимацию стационарного состояния кровотока и транспорта веществ в ткани при различных значениях скорости потребления кислорода тканями.

При переходе человека из одного стационарного состояния к другому (например, от состояния легкой физической нагрузки к интенсивной физической нагрузке или наоборот) все биохимические и прочие процессы переходят из одного стационарного состояния в другое. В ходе численных экспериментов на компьютере было рассчитано время необходимое для стабилизации процессов при переходе от начальных условий (отсутствие кислорода и продуктов метаболизма в ткани) к стационарным условиям, а также при переходе от легкой физической нагрузки (W = 10 мл/100 г/мин) к интенсивной (W = 20 мл/100 г/мин) и обратно.

Были получены аппроксимационные формулы для U и t относительно ΔP и W

$$t = a\,\Delta P\,W - b\,W - c\,\Delta P + d, \quad U = e\,\Delta P + f - \frac{g\,\Delta P + h}{W^2} \tag{10}$$

где $a = 0{,}0016$, $b = 0{,}248$, $c = 0{,}037$, $d = 6{,}085$, $e = 0{,}006$, $f = 0{,}35$, $g = 0{,}267$, $h = 37{,}0$.

Расчеты на компьютере позволили оценить время стабилизации процессов в системе микроциркуляции при переходе от легкой физической нагрузки (W = 10 мл/100 г/мин) к тяжелой (W = 20 мл/100 г/мин) и обратно. Эти результаты показывают, что время стабилизации переходных процессов от начальных условий, соответствующих легкой физической нагрузке (W = 10 мл/100 г/мин), к интенсивной физической нагрузке (W = 20 мл/100 г/мин) составляет 0,6–0,7 мин при артерио-венозной разности давлений 75–105 mm Hg. При переходе от интенсивной физической нагрузки к легкой физической нагрузке требуется 1,7–2,4 минут. Расчетные результаты сравнивались с экспериментально наблюдаемыми временными ответами в микрососудистом ложе, которые составляют около 2–4 мин [1]. Сравнение времени перехода от легкой к интенсивной физической нагрузке и обратно показывает, что в последнем случае время перехода больше в 2,8–3,4 раза.

Таким образом, модель дает хорошую аппроксимацию времени стабилизации процессов в ткани в зависимости от скорости потребления кислорода тканью и разности давлений на концах сосудистого русла.

Заключение. Построена математическая модель регуляции кровотока и транспорта кислорода вазоактивными продуктами метаболизма, учитывающая строение сосудистого русла (артерии, артериолы, капилляры, венулы, вены), диаметры и длины сосудов, вязкость крови, разность давлений на концах сосудистого русла, размеры эритроцита, слой между эритроцитом и тканью (плазма, эндотелий, интерстициальное пространство), производство продуктов метаболизма в ткани, транспорт кислорода из эритроцитов в ткань и продуктов метаболизма из ткани в сосудистое русло, влияние вазоактивных продуктов метаболизма на мышцы артериол и, следовательно, на диаметры артериол, скорость кровотока и транспорт кислорода в ткани. На основе построенной модели дана постановка задачи о стационарных режимах кровотока и транспорта кислорода, позволяющая численно оценить скорость кровотока, диаметры артериол, перепады давлений в сосудах при различных значениях скорости потребления кислорода тканями, которая зависит от степени физической нагрузки на организм. Найдены аппроксимационные формулы времени перехода системы транспорта кислорода из одного стационарного состояния в другое в зависимости от скорости потребления кислорода тканями, разности давлений на концах сосудистого дерева, скорости кровотока. Выявлено значение скорости потребления кислорода тканями (W). Показано, что при переходе от легкой физической нагрузки ($W = 10$ мл O_2/100 г/мин) к интенсивной ($W =$ 20 мл O_2/100 г/мин), время затрачиваемое на переходные процессы во втором случае больше в 2,6–3,4 раза, чем в первом случае. При увеличении W в 2 раза скорость кровотока возрастает в 2,2–2,8 раза, что соответствует экспериментальным данным (в 2–3 раза).

Наибольший интерес представляет измерение концентрации продуктов метаболизма в артериоле, поскольку концентрация является определяющим фактором для диаметра артериол. В случае кратковременного выброса продуктов метаболизма, информация с интерорецепторов о локальном повышении концентрации продуктов метаболизма может привести либо к резкому сужению артериол, либо к резкому их расширению. В обоих случаях это может привести к

необратимым последствиям, например, либо к спазмам сосудов, либо к резкому понижению давления, что в свою очередь может привести к летальному исходу.

СПИСОК ЛИТЕРАТУРЫ

1. Копыльцов А.В. Математическое моделирование кровотока и транспорта кислорода в нормальных и экстремальных условиях. Диссертация на соискание ученой степени доктора технических наук / Санкт-Петербург, 1996, 297 с.
2. Копыльцов А.В. Математическое моделирование кровотока и транспорта кислорода в нормальных и экстремальных условиях. Автореферат диссертации на соискание ученой степени доктора технических наук / Санкт-Петербург, 1996, 32 с.
3. Копыльцов А.В. Математическое моделирование транспорта кислорода в человеческом организме. В кн.: «Телемедицина» (ред. Юсупов Р.М. и Полонников Р.И.). СПБ: СПИИРАН, 1998, с. 323–366.
4. Копыльцов А.В. Математическое моделирование транспорта кислорода в сердечно-сосудистой системе человека. В журнале: Вестник СПбО РАЕН, 1999, № 3(4), с.381–387.
5. Копыльцов А.В. Математическое моделирование и система микроциркуляции. СПБ: ЛГОУ, 2000, 112 с.
6. Копыльцов А.В. Математическое моделирование локальной регуляции кровотока // Вестник Нижневартовского государственного гуманитарного университета. 2013, № 1, С. 37–42.
7. Kopyltsov A. V. Mathematical model of the motion of asymmetric erythrocytes along narrow capillaries // Russian Journal of Numerical Analysis and Mathematical Modelling, 2012, T. 26, № 6, C.535–553.
8. Kopyltsov A.V., Groebe K. Mathematical modeling of local regulation of blood flow by veno-arterial diffusion of vasoactive metabolites. In: Oxygen transport to Tissue XVIII , edited by Nemoto and LaManna, Plenum Press, New York, 1997, pp.303–311.

УДК 004.05

РЕАЛИЗАЦИОННЫЕ ОСНОВЫ СИГНАТУРНО-ЭВРИСТИЧЕСКОГО АНАЛИЗА БЕЗОПАСНОСТИ ПРОГРАММ

Марков Алексей Сергеевич, Фадин Андрей Анатольевич,
ЗАО «НПО «Эшелон»,
Россия, Москва, ул. Электрозаводская, д. 24,
e-mails: am@cnpo.ru; mail@cnpo.ru

Аннотация: Описано применение статического анализа для обнаружения уязвимостей и дефектов программного кода. Показано, что полноту проверок можно осуществить, используя предлагаемый сигнатурно-эвристический анализ безопасности программного кода. Рассмотрены вопросы формального описания сигнатурно-эвристического анализа безопасности программного кода. Дано описание программной реализации статического анализатора. Представлены результаты оценки его эффективности.

Ключевые слова: *безопасность программ; дефекты безопасности; уязвимости; эвристический анализ; недекларированные возможности.*

IMPLEMENTAL BASICS OF SIGNATURE-HEURISTIC ANALYSIS OF SECURITY SOFTWARE

Alexey S. Markov, Andrei A. Fadin,
NPO Echelon,
Russia, Moscow, Elektrozavodskaya ul, 24,
e-mails: am@cnpo.ru; mail@cnpo.ru

Abstract: The application of static code analysis to detect vulnerabilities and weaknesses in software code is analyzed. It is shown that the completeness of checks can be carried out using the proposed analysis of the security code. The problems of the formal description of the signature-heuristic analysis of security software are considered. The description of the software of static analyzer is presented. The results of the evaluation of its effectiveness are shown.

Keywords: *software security; weakness; vulnerability; heuristic analysis; undeclared capabilities.*

Введение. 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 [1]. 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 [2], [3].

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 [4]. 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 [5], [6], являющийся открытым, исчерпывающим источником информации о дефектах. Средства CppCat и CppCheck позволяют проводить ревью 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 [2].

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) [7].

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 [8].

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 [9], [10], [11].

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Юсупов Р.М. Текущее состояние и тенденции развития в области построения безопасных компьютерных систем // В сборнике: 5-я Российская мультиконференция по проблемам управления материалы конференции «Информационные технологии в управлении» (ИТУ-2012). 2012. С. 671–675.
2. Аветисян А.И., Белеванцев А.А. Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения. // Вопросы кибербезопасности. 2014. № 3 (4). С. 20–28.
3. Медведев Н.В., Марков А.С., Фадин А.А. Применение метода статического сигнатурного анализа для выявления дефектов безопасности веб-приложений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. № 9. С. 21–25. DOI = http://dx.doi.org/10.7463/0912.0461281
4. Марков А.С., Фадин А.А. Проблемы автоматизации выявления программных закладок и дефектов безопасности кода методом статического сигнатурного анализа // В сборнике: 5-я Российская мультиконференция по проблемам управления материалы конференции «Информационные технологии в управлении» (ИТУ-2012). 2012. С. 717–722.
5. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3 (51). С. 56–61.
6. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы уязвимостей // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 11. С. 62–67.
7. Марков А.С., Фадин А.А., Цирлов В.Л. Концептуальные основы построения анализатора безопасности программного кода // Программные продукты и системы. 2013. № 1. С. 10.
8. Barabanov A., Markov A., Fadin A., Tsirlov V. A production model system for detecting vulnerabilities in the software source code. In Proc. SIN '15. September 08-10, 2015, Sochi, Russian Federation. DOI= http://dx.doi.org/10.1145/2799979.2800019
9. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42–48.
10. Markov, A., Luchin, D., Rautkin, Y., Tsirlov, V. 2015. Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements, In Proceedings of the 11th International Siberian Conference on Control and Communications (Omsk, Russia, May 21-23, 2015). SIBCON-2015. IEEE, Omsk, Russia, 1–4. DOI = http://dx.doi.org/10.1109/SIBCON.2015.7147139
11. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (3). С. 36–39.

УДК 004.6; 004.08

ОРГАНИЗАЦИЯ МЕТАДАННЫХ ПРИ ДЛИТЕЛЬНОМ ХРАНЕНИИ ИНФОРМАЦИИ

Пойманова Екатерина Дмитриевна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mail: e.d.poymanova@gmail.com.

Аннотация: обсуждается проблема организации специализированной адресной системы, позволяющей пользователям сохранить и осуществлятьпоиск информации. Специфика задачи заключается во временной разнице между создателем информационного ресурса и его пользователем.

Ключевые слова: *данные; метаданные; сохранение данных; длительное хранение; адресная система; стандарт организации метаданных.*

ORGANIZATION OF METADATA WITH LONG-TERM INFORMATION STORAGE

Poymanova Ekaterina
Saint-Petersburg State University of Economics
Russia, St. Petersburg,Sadovaya str., 21,
e-mail: e.d.poymanova@gmail.com

Abstract: is discussed the problem of organizing specialized addressing system that allows users to save and search for information. The specificity of the problem lies in the temporary difference between the creator of the information resource and its user.

Keywords: data; metadata; saving data; long-term storage; address system; a metadata standard.

Введение. Понятие «информационная безопасность» включает в себя помимо прочего безопасность хранения данных и организацию доступа к ним. При длительном хранении информации (срок может варьироваться от 70 до нескольких тысяч лет) остро встает проблема организации адресной системы, которая позволила бы одним пользователям сохранить информацию, адругим найти ее и воспользоваться ею, даже если временной интервал между сохранением и необходимостью доступа к такой информации составляет несколько поколений[1].

Задача организации такой адресной системы первым делом приводит к проблеме организации структуры метаданных. Без них нельзя преобразовать цифровые данные (материальный уровень) в аналоговые – 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 [2].

1. Этапы процесса сохранения данных. Процесс сохранения данных можно представить следующей схемой, приведенной на рисунке 1. Инициатива – первый этап сохранения информации. На данном этапе у пользователя (инициатора хранения) возникает необходимость в долговременном хранении информации. Инициатором может выступать любое юридическое или физическое лицо.

Анализ информации – на данном этапе инициатор и некий технический специалист формируют первичные метаданные (тип информации, ее содержание, требования ко времени хранения, требования к ограничению доступа и др.). Запись информации на носитель – на данном этапе происходит сжатие, кодирование информации и запись ее на физический носитель. Также формируются технические метаданные, такие как формат хранимой информации, тип носителя, условия хранения носителя и т.д. Размещение носителя в архиве – физическое размещение носителя в специальных условиях (в зависимости от типа носителя), присвоение носителю физического адреса. На данном этапе возникает необходимость занесения метаданных, включая физический адрес носителя, в специализированную базу метаданных.

Хранение носителя – поддержание специальных условий хранения для различных видов носителей, обеспечивающих хранение данных на этом носители в течение установленного срока. На данном этапе может вестись регистрация состояния носителя и изменение элемента метаданных «Статус носителя» (см. ниже список элементов).

Предоставление информации пользователю – на данном уровне должен быть организован процесс предоставления хранимой информации пользователю, реализовано разграничение доступа, организован собственно процесс преобразования цифровых данных в аналоговые (например, визуализация информации).

Удаление информации – срок хранения информации может быть ограничен по желанию инициатора, по окончанию срока хранения носитель информации, на котором содержатся данные изымается из архива и утилизируется. В данном случае в базу метаданных заносится информация об

уничтожении носителя и информации. Содержание метаданных должно однозначно идентифицировать объект (данные) как по смысловой нагрузке, так и по физическому расположению носителя.

2. Стандарт метаданных. В настоящее время существуют различные стандарты метаданных, в зависимости от предметной области. Для описания метаданных сетевых ресурсов был создан и широко применяется стандарт «Дублинское ядро» (DublinCore). Стандарт содержит ряд элементов, представляющих собой два уровня: простые и компетентные элементы, а также содержит ряд уточнений, которые могут быть полезны для обнаружения ресурсов [3].

Стандарт содержит следующие элементы:

Простые:

– Title (заголовок);
– Creator (создатель);
– Subject (тема);
– Description (описание);
– Publisher (издатель);
– Contributor (принявший участие);
– Date (дата);
– Type (тип);
– Format (формат документа);
– Identifier (идентификатор);
– Source (источник);
– Language (язык);
– Relation (отношения);
– Coverage (зона охвата) - обычно включает пространственное положение (название местности или географические координаты), временной период или юрисдикцию (например, указание единицы административного деления);
– Rights (авторские права).
– Компетентные:
– Audience — аудитория;
– Provenance — происхождение;
– RightsHolder — правообладатель.

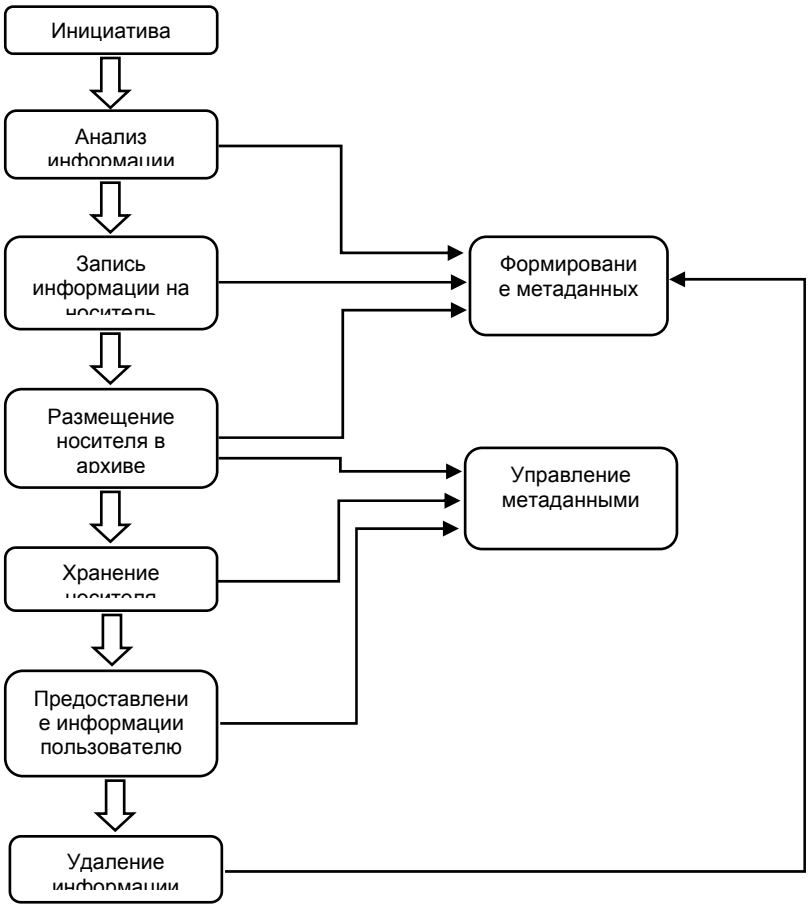


Рис.1 Схема процесса сохранения данных

Стандарт «Дублинское ядро» может послужить основой системы метаданных для информации длительного хранения.

Поскольку речь идет о самых разнообразных данных, хранящихся веками, имеет смысл дополнить список элементов метаданных стандарта «Дублинское ядро» такими элементами, как:

– предполагаемое время хранения;
– статус (хранится, подготавливается к удалению, удалена);
– данные о носителе информации;
– данные об ограничении доступа;
– оборудование для считывания данных и др.

Помимо этого, остро встает вопрос о лице, формирующем метаданные, а также об управлении ими. Лицо, формирующее метаданные должно с одной стороны, обладать достаточной квалификацией чтобы отразить технические характеристики данных, а с другой стороны, в достаточном объеме владеть информацией, которую необходимо сохранить, чтобы сформировать описательную часть элементов метаданных.

Логично предположить, что создавать метаданные должны как минимум два лица:

– собственник информации – может формировать ту часть элементов метаданных, которая относится к описанию самих данных, предполагаемому сроку хранения, ограничениям доступа;

– технический специалист – может формировать часть элементов метаданных, касающуюся технических аспектов хранения информации, таких как носитель, формат, оборудование для считывания данных. Для организации управления метаданными должна быть разработана модель базы метаданных, которая обеспечила бы хранение, управление и своевременное обновление метаданных информации длительного хранения[4].

Метаданные можно классифицировать по указанным ниже признакам.

1. 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).

2. По необходимости формирования:

– обязательные (необходимые для идентификации и чтения информации);
– желательные (заявленные инициатором хранения).

3. По месту хранения:

– хранимые на носителе вместе с информацией;
– хранимые в базе метаданных.

Итак, метаданные необходимы для преобразования аналоговой информации (воспринимаемой органами чувств) в цифровые данные для записи на физический носитель и обратного преобразования цифровых данных в аналоговые.

Если провести аналогию с эталонной моделью взаимодействия открытых систем, можно сказать, что информация, проходя приведенные выше этапы сохранения, проходит своеобразную процедуру инкапсуляции, «обрастая» различными метаданными [5],[6]. В таблице 1 приведены этапы сохранения информации и примеры метаданных, формируемых на данных этапах.

Таблица 1

Этап сохранения	Формируемые метаданные	Кто выполняет
Предоставление информации в аналоговом виде	-	Инициатор хранения
Анализ информации – формирование первичных метаданных	Title (заголовок); Creator (создатель); Subject (тема); Description (описание); Date (датасоздания); Storagetime(предполагаемое время хранения) данные об ограничении доступа и т.д.	Инициатор хранения совместно с техническим специалистом
Перевод аналоговой информации в цифровую	Формат данных; размер файлов; количество файлов; местоположение файлов на носителе и т.д.	Технический специалист
Сжатие, шифрование, запись на носитель	Тип носителя; характеристики оборудования для считывания информации и т.д.	Технический специалист
Размещение носителя в архиве	Местоположение носителя в хранилище; географические координаты хранилища.	Технический специалист

Заключение. Формирование метаданных при сохранении ведет за собой и заполнение базы метаданных. Поскольку количество производимой информации растет в геометрической прогрессии логично предположить, что количество информации длительного хранения также будет расти высокими темпами. Следовательно, становится актуальной задача минимизации количества метаданных, хранимых в базе метаданных. Для этого необходимо большую часть метаданных хранить на самих носителях, меньшую часть – в локальных базах метаданных конкретного хранилища (например, данные о местоположении носителя информации) и минимум метаданных в глобальных базах (в идеальном случае должна быть одна национальная база таких метаданных).

СПИСОК ЛИТЕРАТУРЫ

1. Пойманова Е.Д. Современные технологии сохранения информации//Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)», Санкт-Петербург, 2013 г.
2. Татарникова Т.М., Пойманова Е.Д.Технологии долговременного хранения данных//Материалы международной научно-практической конференции «Наука и образование в XXI веке», часть 31, Тамбов, 2013. С. 136-138.
3. Спецификация стандарта Дублинское ядро http://dublincore.org/documents/usageguide/elements.shtml
4. Головкин Ю.Б., Гусаренко А.С., Информационная система кредитования юридических лиц в банке // Актуальные инновационные исследования: наука и практика. 2010. № 3. С. 14.
5. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель обработки клиентских запросов//Телекоммуникации. 2013. №9. С. 42-48.
6. Аль-Хаками Али Мохаммед Омар,Татарникова Т.М. Оценка вероятностно-временных характеристик сетей хранения данных SAN//Программные продукты и системы. 2009. №4. С. 177-179.

УДК 004.6; 004.08

УСЛУГИ ДЛИТЕЛЬНОГО ХРАНЕНИЯ ДАННЫХ

Пойманова Екатерина Дмитриевна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mail: e.d.poymanova@gmail.com.

Аннотация: В статье рассматриваются технические аспекты возможности предоставления услуг длительного хранения данных, а также физические принципы сохранения. Приводятся энергетические, пространственные и временные характеристики различных носителей информации.

Ключевые слова: *информационный процесс сохранения данных; носитель информации; технология сохранения; время хранения; плотность записи; энергетический барьер.*

SERVICES OF LONG TERM STORAGE

Poymanova Ekaterina,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: e.d.poymanova@gmail.com.

Abstract: The article discusses the technical aspects can provide services long-term storage of data, and the physical principles of conservation. Provides energy, spatial and temporal characteristics of different media.

Keywords: *information process of storing data; media; technology preservation; storage; recording density; the energy barrier.*

Введение. Понятие «информационная безопасность» включает в себя помимо прочего безопасность хранения данных и организацию доступа к ним. Информатизация ставит новые задачи перед предприятиями сервиса. Одной из таких задач является предоставление услуг по долговременному хранению данных. Пользователями подобных услуг могут быть и юридические, и физические лица. Первые из них должны сохранять большие объемы персональных и экономических данных в соответствии с законодательством РФ (до 70-ти лет), а также технологические данные, которые могут быть востребованы по мере развития их бизнеса. Вторые заинтересованы, например, в долговременном хранении видео и фото архивов, которые требуют больших объемов запоминающих устройств и не могут быть надежно сохранены на широко доступных информационных носителях в домашних условиях.

В работе [1] выделены базовые информационные процессы, к числу которых отнесен и процесс сохранения информации. Согласно [1] сохранение данных может быть представлено на двух метауровнях: смысл и данные.

С философской точки зрения метауровень «смысл» является идеальным уровнем. Измерить смысл, передающийся между коммуникантами не представляется возможным – для него не существует объективных оценочных характеристик. Метауровень «данные», в свою очередь,

является материальным уровнем. Данные, по сути являясь набором цифр и всегда передаются между устройствами, при этом для устройств, участвующих в процессе сохранения, носителей данных и для самих данных существуют четко определенные характеристики.

Особенностью процесса сохранения является функция переноса данных во времени, поэтому его основными характеристиками являются:

tc – время сохранения, должно быть максимальным;

A – количество или V – объем сохраненных данных;

E – энергетический барьер, который необходимо преодолеть, чтобы изменить значение бита.

1. Принцип сохранения цифровых данных. Принцип сохранения данных основан на понятии минимальной единицы хранения (МЕХ), способной оставаться в одном из нескольких устойчивых состояний. От количества состояний зависит количество бит, которые можно сохранить в МЕХ: если МЕХ имеет 2 устойчивых состояния, то может сохранить 1 бит данных, если 4, то – 2 бита, если 8, то – 3 бита и т.д.

Очевидно, что от количества состояний МЕХ зависит такая важная характеристика как плотность.

Физически принцип сохранения может быть реализован следующими способами:

1. Магнитная запись. Носителями информации являются магнитная лента и магнитный диск. Минимальной единицей хранения является домен (макроскопическая область, в которой ориентация вектора спонтанной однородной намагниченности определенным образом повернута или сдвинута относительно направлений соответствующего вектора в соседних доменах).

2. Полупроводниковая запись. Носителем информации является твердотельный накопитель (SSD – solid-state drive). Минимальной единицей хранения является триггер (класс электронных устройств, обладающих способностью длительно находиться в одном из двух устойчивых состояний и чередовать их под воздействием внешних сигналов).

3. Механическая (оптическая) запись. Носителями информации являются различные оптические диски (CD, DVD, BD, M диск, стеклянный диск). Минимальной единицей хранения является информационный рельеф (спиральная дорожка, состоящая из череды ямок (питов – pits) и промежутков между питами (лэндов – lands); переход от лэнда к питу и наоборот обозначает единицу, а длина пита или лэнда – длину серии нулей).

4. Вольфрамовый диск. Носителем является вольфрамовый диск, являющийся по сути оптическим носителем. Информация на такой диск записывается с помощью QR-кодов. Минимальной единицей хранения для такого носителя является QR-код.

5. Магнитооптическая запись. Носителями информации являются магнитооптические диски (MO диски). Минимальной единицей хранения является домен.

6. Биологическая запись. Носителями информации является биоматериал или бактерии. Минимальной единицей хранения является молекула ДНК.

2. Классификация носителей информации. Характеристики различных носителей (время хранения, объем данных на одном носителе, плотность записи и энергетический барьер) различаются и зависят как от применяемой технологии, так и от материала носителя.

В таблице 1 приведены характеристики различных типов носителей информации. Для каждого носителя отобраны лучшие значения характеристик, достигнутые в той или иной технологии (временя хранения, объем данных на носителе и плотность записи), в том числе указаны характеристики прототипов носителей.

Таблица 1

Вид носителя	Характеристика			
	Время хранения (t_c), лет	Объем данных на одном носителе ($V_н$), байт	Плотность записи (ρ), бит/(дюйм)^2	Энергетический барьер
Магнитный диск [2], [3]	5	6 442 450 944 (6 ТБ)	643 000 000 000	$1{,}44113*10^{-19}$
Магнитная лента [4], [5], [6]	50	4 294 967 296 (4 ТБ)	29 500 000 000	$1{,}32896*10^{-19}$
Твердотельный накопитель [7], [8], [9], [10]	100	10^9	~ 593 883 752	$1{,}23988*10^{-19}$
CD [11]	100	921 600 (900 МБ)	~ 421 365	$9{,}50372*10^{-20}$
DVD (двуслойный двусторонний DVD-18)	100	17 825 792 (17 ГБ)	~ 8 150 137	$1{,}07307*10^{-19}$
BD (четырехслойный)	100	134 217 728 (128 ГБ)	~ 61 365 742	$1{,}15669*10^{-19}$
M-диск (DVD) [12]	10^3	4 928 307 (4,7 ГБ)	~ 2 253 273	$9{,}24445*10^{-20}$
M-диск (BD) [12]	10^3	26 214 400 (25 ГБ)	~11 985 497	$9{,}93672*10^{-20}$
Стеклянный диск [13]	10^6	386 547 056 640 (360 ТБ)	~ 176 733 337 278	$1{,}10513*10^{-19}$
Вольфрамовый диск (QR-код) [14]	10^6	~ 1 048 576 (1 ГБ)	~ 479 420	$5{,}74217*10^{-20}$
Магнитооптический накопитель (5,25 дюйма) [15]	50	9 542 042 (9,1 ГБ)	~ 3 526 329	$1{,}0759*10^{-19}$
1 грамм биоматериала [16]	50	$2{,}2\cdot10^{12}$ (2,2 ПБ)	$17{,}6\cdot10^{12}$ бит на гамм	$1{,}58738*10^{-19}$
Бактерии (1 грамм) [17]	10^3	94 371 840 (90 ГБ)	754 974 720 бит на грамм	$1{,}04673*10^{-19}$

Энергетические характеристики получены по выражению (3).

Характеристика рассчитана исходя из технических данных, приведенных в [9] и [10].

Для всех оптических дисков характеристика «плотность записи» является расчетной.

3. Расчет энергетического барьера. Рольф Ландауэр в 1961 г. показал, что расход энергии в процессе вычислений связан с уничтожением битов данных, и сформулировал следующий принцип: «Независимо от физики и технологии вычислительного процесса при потере 1 бита данных в процессе вычисления как минимум выделяется энергия, равная

$$E=k_B \cdot T \cdot \ln 2, \ (Дж) \qquad (1)$$

где k_B – постоянная Больцмана, определяющая связь между температурой и энергией (~ $1{,}3807 \cdot 10^{-23}$ Дж/К);

T – температура, при которой ведутся вычисления (T = 300K = 26,85°C).

Остальные операции (копирование, установка, перенос и др.) требуют сколь угодно мало энергии при достаточно малой скорости протекания.

В статье Лажио Киш и Кио Гранквист «Имеет ли информация массу?» [18] показано, что минимальную энергию, необходимую для преодоления энергетического барьера можно рассчитать следующим образом:

$$E > k_B T \ln\left(N \frac{t_m}{\tau}\right), \qquad (2)$$

где k_B – постоянная Больцмана

T – абсолютная температура окружающей среды

N – количество бит, содержащееся в памяти

t_m – время жизни памяти

τ – время корреляции тепловых флуктуаций от термического возбуждения.

Заменим отношение (t_m/τ) на отношение ($t_п/t_н$), где $t_п$ – время хранения, необходимое пользователю, $t_н$ – время хранения, обеспечиваемое конкретным носителем.

Тогда формула для нахождения энергии, необходимой для преодоления энергетического барьера имеет следующий вид:

$$E > k_B T \ln\left(N \frac{t_п}{t_н}\right). \qquad (3)$$

Физический смысл отношения ($t_п/t_н$) – количество циклов перезаписи информации в течение времени хранения, заданного пользователем.

Таким образом можно рассчитать энергию, затрачиваемую на преодоления энергетического барьера для рассматриваемых носителей.

При расчетах были приняты следующие значения характеристик:

k_B – постоянная Больцмана, k_B=$1{,}3807 \cdot 10^{-23}$ Дж/К;

T – температура окружающей среды, T=300K;

$t_п$ – время хранения, необходимое пользователю, $t_п$ =1 000 000 лет – это наибольшее время хранения, обеспечиваемое современными носителями информации.

4. Ресурсная модель базовых информационных технологий. Для описания ресурсного обеспечения базовых информационных технологий может быть использован параллелепипед (рис. 1), грани которого отображают нижние и верхние границы пространства, времени и энергии, необходимые информационным технологиям на некотором этапе их развития [19].

В этой модели ось ординат (S) отображает пространственные, ось аппликат (F) – энергетические, ось абсцисс (T) – временные параметры технологии.

Точки, лежащие в пределах объема параллелепипеда и имеющие координаты 0≤S≤Smax, 0≤T≤Tmax, 0≤F≤Fmax, соответствуют некоторым уже реализованным или еще разрабатываемым технологиям. В качестве примера рассмотрим технологии сохранения больших данных, которым также требуются все большие объемы физических ресурсов. При этом необходимо учитывать требования, в том числе к:

– плотности записи, поскольку от нее зависят размеры и количество носителей;

– величине гарантированного времени сохранения данных;

– величине энергозатрат, которые необходимы для записи/считывания данных на носитель и для защиты носителя от внешних воздействий между моментами записи и считывания.

Перечисленные пространственные, временные и энергетические параметры цифровых технологий сохранения зависят друг от друга. Улучшение любого из них может быть, как правило, достигнуто только за счет ухудшения других. Это хорошо демонстрируют, например, технологии полупроводниковой памяти SLC, MLC, TLC, в которых увеличение плотности записи достигается за счет снижения гарантированного времени хранения. То же самое можно отнести и к магнитной памяти, где увеличение плотности (уменьшение площади доменов) ведет к появлению взаимного влияния магнитных полей и, соответственно, снижает гарантированное время хранения и

увеличивает энергетические затраты для защиты (восстановления) данных в процессе хранения. Полупроводниковая память характеризуется малым энергопотреблением по сравнению с магнитной, но, заменяя магнитную память полупроводниковой, следует учитывать, что за экономию энергии придется заплатить меньшим временем гарантированного хранения. Уменьшение энергопотребления дисковыми массивами возможно за счет остановки или уменьшения скорости вращения дисков, но это увеличивает время доступа к данным и т.д.

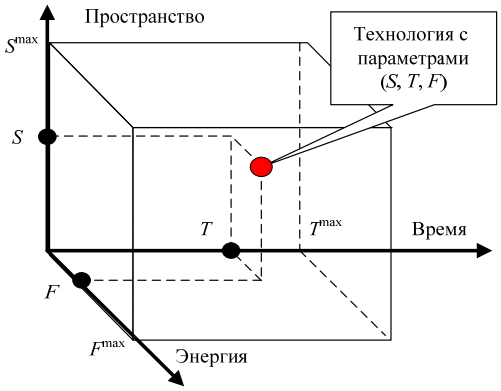


Рис. 1. Модель физических ресурсов информационных процессов

В общем случае, эффективность технологии сохранения тем выше, чем больше плотность и гарантированное время хранения данных и меньше затрачиваемая при этом энергия.

В качестве базовых технологий для долговременного сохранения данных могут использоваться магнитные диски и ленты, полупроводниковая память, компакт и М-диски и др. В каждом из этих технологических сегментов существует множество альтернативных реализаций, в том числе, и у разных производителей. Проведенные исследования показали, что каждая технология характеризуется собственными физическими параметрами:

– магнитные диски обеспечивают высокую плотность, но малое время хранения;

– магнитные ленты гарантируют длительное время хранения, но характеризуются и сравнительно значительным временем доступа;

– полупроводниковая память позволяет экономить энергию, но не способна на долговременное хранение;

– компакт-диски гарантируют длительное время хранения, но имеют ограниченную плотность записи;

– М-диски наиболее долговечны, но энергозатратны в процессе записи и т.д.

Примерами технических решений принятых и реализованных при сохранении больших данных могут служить следующие системы.

Большой адронный коллайдер является источником огромного количества научных данных о результатах столкновений элементарных частиц. Оцифрованные данные только о тех столкновениях, которые дали интересные с точки зрения физики результаты, поступают со скоростью около 50 событий в секунду. В главном центре хранения и обработки эти данные записываются на магнитную ленту. К настоящему времени на десятках тысяч картриджей уже собрано более 100 Пбайт данных. Доступ к картриджам автоматизирован: они хранятся в специальных подвальных помещениях на полках, откуда их достает робот. Энергопотребление системы хранения составляет 3.5 МВт. Фрагменты данных копируются на перекрывающий кэш диска для доступа и распределения между исследовательскими центрами по всему миру. Особенности данной системы – это отсутствие жестких ограничений на время обработки данных, что позволяет уменьшить энергозатраты.

Другой пример – это система долговременного хранения данных ColdStorage компании Facebook. Она располагается в отдельном здании и оптимизирована с точки зрения уменьшения энергопотребления и увеличения плотности размещения данных, а не производительности и доступности. Для этого используются магнитные диски, которые не рассчитаны на постоянную эксплуатацию, но позволяют менять скорость вращения, увеличивать количество дисков в одной стойке и уменьшать количество одновременно вращающихся дисков. В результате выбора именно такой технологии хранения для энергопитания массива дисков емкостью 1 Эбайт требуется примерно 0,375 МВт вместо 1,5МВт.

Еще одно решение от Facebook – это экспериментальное хранилище, которое состоит из трехсот тысяч оптических дисков, где хранятся 30 Пбайт данных. Нужный диск с требуемыми файлами находит робот. В перспективе система оптического хранения сможет сохранять до 150 Пбайт. Эта система заметно увеличивает время доступа к затребованным файлам, но позволяет увеличить гарантированное время сохранения и на 80 % снизить энергопотребление.

Выбор того или иного решения должен основываться на использовании обобщенного критерия или сравнении доступных технологий друг с другом по всем физическим характеристикам, которые

могут быть отображены в виде параллелепипеда, подобного представленномуна рис. 2. В процессе такого сравнения следует, используя принцип Парето, удалить из рассматриваемого набора такие технологии, которые заведомо хуже других по пространственным, временными и энергетическим характеристикам в совокупности. Если количество технологий, превосходящих другие хотя бы по одному показателю, останется достаточно много, то следует применить один из методов многокритериального выбора. Набор параметров задачи оптимизации зависит, при этом, от вида базовой технологии сохранения данных. Оптимизируемыми параметрами могут являться, например, скорость вращения и количество одновременно вращающихся дисков, плотность дисков на стойке, пространственные, временные и энергетические характеристики робототизированных систем, объемы сохраняемых данных и другие параметры. Критериями эффективности можно выбирать потребляемые физические ресурсы системы, а в качестве ограничений – вероятностно-временные характеристики производительности и доступа, размеры производственных помещений, возможности силовых агрегатов и т.п. Предложенный подход развивает традиционные схемы оптимизации производительности информационных систем за счет выбора числа обслуживающих устройств, их быстродействия и надежности без учета объемов потребляемых при этом физических ресурсов и применим к широкому кругу базовых информационных процессов и технологий.

5. Классификация носителей по времени хранения. Поскольку каждый носитель имеет свой ресурс, а любая информация имеет свои требования к длительности хранения, можно выделить следующие интервалы предполагаемых (или желаемых), а также законодательно определенных сроков хранения информации:

- до одного года;
- от 1 года до 10 лет;
- от 10 лет до 100 лет;
- от 100 лет до 1000 и более лет.

Как правило данные, хранящиеся до одного года – это так называемые исходные данные, постоянно использующиеся для обработки. Такие данные как правило хранятся в центрах обработки данных (ЦОД), для них важнейшим показателем является время доступа, которое должно быть минимальным. То есть работа с такими данными происходит в режиме реального времени. В качестве носителя в данном случае целесообразно использовать RAID массивы, которые могут обеспечить минимальное время доступа.

Следующий тип данных с точки зрения времени хранения – это резервные копии. Время их хранения обычно составляет от 1 года до 10 лет. 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 (СХД), 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. От 10 до 100 лет хранятся архивные данные. В данном случае целесообразно использовать CD/DVD/BD библиотеки и библиотеки, основанные на М-дисках, также возможно применение твердотельного накопителя. И последний тип данных с точки зрения времени хранения – 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.

Проведенные исследования позволили классифицировать носители информации в зависимости от физического типа памяти и временного ресурса, что приведено в таблице 2.

Таблица 2

Классификация носителей информации в зависимости от ф
изического типа памяти и временного ресурса

Срок хранения, лет	Магнитная запись	Магнитооптическая запись	Механическая запись	Полупроводниковая память	Биологическая память
>1000			Вольфрамовый диск до 1 000 000 лет Стеклянный диск до 1 000 000 лет		
100-1000			М (DVD/BD) диск до 1 000 лет		ДНК (бактерии) до 1 000 лет
10-100	Магнитная лента до 30 лет	Магнитооптический диск до 50 лет	CD/DVD/BD до 100 лет	Твердотельный накопитель до 100 лет	ДНК (биоматериал)
1-10	Магнитный диск до 5 лет Магнитная лента до 30 лет	Магнитооптический диск до 50 лет	CD/DVD/BD до 100 лет	Твердотельный накопитель до 100 лет	

Заключение. Выявленный тренд развития базовых информационных технологий показывает, что учет затрат на обеспечение информационных технологий физическими ресурсами становится существенным при проектировании мощных информационных систем таких как, например, системы хранения данных, центры обработки данных или суперкомпьютеры. Их эффективность зависит не только от возможностей информационных технологий в части объемов хранения, скорости передачи и обработки данных, но и от объемов занимаемого пространства, временных параметров физических процессов и потребляемой энергии. Поэтому при проектировании подобных информационных систем следует:

– рассматривать весь спектр доступных информационных технологий сохранения, распространения и обработки;

– учитывать в процессе выбора физические параметры технологий;

– согласовывать физические параметры технологий с допустимыми параметрами задач пользователя,

– учитывать взаимную зависимость пространственных, временных и энергетических характеристик технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность.– 2014.– №1(25).–С.69–77.
2. Спецификация жестких дисков фирмы HGST, a Western Digital company http://www.hgst.com/tech/techlib.nsf/techdocs/83F507776F03BE7C88257C37000AED30/$file/USHe6_ds.pdf
3. Технические характеристики жесткого диска Enterprise Capacity 3.5 HDD SAS 512E SED FIPS 6 ТБ http://www.seagate.com/ru/ru/internal-hard-drives/enterprise-hard-drives/hdd/enterprise-capacity-3-5-hdd/#specs
4. Обзор IBM System Storage TS1140 Tape Drive http://www-03.ibm.com/systems/ru/storage/tape/ts1140/
5. Обзор продуктов IBM System Storage http://www-03.ibm.com/systems/ru/resources/6452_IBM_Sys_Storage_Product_Guide_Product_Guide_TSO00364-RURU-46_Final_Mar12_13.pdf
6. IBM Research: новый рекорд плотности записи данных на магнитную ленту http://www.thg.ru/technews/20100127_002800.html
7. Обзор накопителя SanDisk® Memory Vault http://ru.sandisk.com/products/usb/memory-vault/
8. Обзор накопителя Samsung 1ТБ 2,5" SSD 840 EVO 840 SATA III http://www.samsung.com/ru/consumer/memory-storage/ssd/840-evo/MZ-7TE1T0BW
9. Обзор https://www.hardwareluxx.ru/index.php/news/hardware/festplatten/24953-micron-smallest-128-gb-nand-flash-soon-in-ssds.html+&cd=1&hl=ru&ct=clnk&gl=ru
10. Обзор http://www.3dnews.ru/791909
11. http://www.etilux.com/en/product/cd-38/verbatim-cd-r-7207.php
12. Сайт производителя М-дисков http://www.mdisc.com/what-is-mdisc/
13. Jingyu Zhang, Mindaugas Gecevičius, Martynas Beresna, Peter G. Kazansky. 5D Data Storage by Ultrafast Laser Nanostructuring in Glass. http://www.orc.soton.ac.uk/fileadmin/downloads/5D_Data_Storage_by_Ultrafast_Laser_Nanostructuring_in_Glass.pdf
14. http://www.utwente.nl/en/newsevents/2013/10/141415/mega-tot-gigajaar-opslagmedium-kan-mensheid-overleven
15. Технические характеристики МО диска на сайте производителя http://www.sony.ru/pro/product/it-storage-media-5-mo-disk/cwo9100/specifications/#specifications
16. Nick Goldman, Paul Bertone, Siyuan Chen, Christophe Dessimoz, Emily M. LeProust, Botond Sipos & Ewan Birney. Towards practical, high-capacity, low-maintenance information storage in synthesized DNA http://www.nature.com/nature/journal/v494/n7435/full/nature11875.html
17. Живая память. Бактерии как носитель информации. http://www.popmech.ru/technologies/11255-zhivaya-pamyat-bakterii-kak-nositel-informatsii/
18. Лажло Киш, Кло Гранквист. Имеет ли информация массу? http://www.physics-online.ru/PaperLogos/16714/%C8%EC%E5%E5%F2%20%EB%E8%20%EC%E0%F1%F1%F3%20%E8%ED%F4%EE%F0%EC%E0%F6%E8%FF.pdf
19. Советов Б.Я., Колбанев М.О., Татарникова Т.М. Модель физических характеристик сигналов//Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)», Санкт-Петербург. –2013.–С.64–65.

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ[4]

Сенцова Алина Юрьевна[1], Машкина Ирина Владимировна[1],
[1] Уфимский Государственный Авиационный Технический Университет (ФГБОУ ВПО «УГАТУ»),
Россия, г. Уфа, ул. К. Маркса, д. 12,
e-mails: sentsova.alina@yandex.ru, maskina.vtzi@gmail.com.

Аннотация: В статье рассматривается возможность расчета оперативного значения уровня риска нарушения информационной безопасности в системе облачных вычислений. Для решения этой

[4] Работа выполнена при финансовой поддержке гранта РФФИ 14-07-00928-а

задачи разработана модель угроз в виде нечетких когнитивных карт и используется механизм искусственной нейронной сети.

Ключевые слова: *система облачных вычислений; расчет риска; искусственная нейронная сеть; прогнозируемый и оперативный риск; нечеткая когнитивная карта.*

THE ARTIFICIAL NEURALNETWORK APPLICATION FOR SECURITY RISK ASSESSMENT IN CLOYD COMPUTING SYSTEMS[1]

Sentsova Alina[1], Mashkina Irina[1],
[1] Ufa State Aviation University (USATU),
Russia, Ufa, K. Marks str. 12,
e-mails: sentsova.alina@yandex.ru, maskina.vtzi@gmail.com.

Abstract: In this article the possibility of calculation of information security risks in cloud computing system is considered. The fuzzy cognitive maps and artificial neural network are used for a solution of this problem.

Keywords: *cloud computing system; fuzzy cognitive map; artificial neural network; information security risk.*

В настоящее время технологии облачных вычислений получили широкое распространение и интенсивно развиваются [1]. С точки зрения информационной безопасности облачные вычисления обладают некоторыми особенностями, связанными с тем, что заказчик не имеет доступа к облачной инфраструктуре вендора. Поскольку удаленные облачные сервисы не контролируются заказчиком, конфиденциальность и целостность обрабатываемых данных заказчика в большой степени зависит от безопасности инфраструктуры вендора. В данной работе анализируется бизнес модель продажи и использования программного обеспечения как услуги. В этом случае вендор разрабатывает web приложения и обеспечивает доступ к ним клиента через интернет. Достоинством данной модели для клиента является отсутствие необходимости затрат на приобретение, установку, техническую поддержку оборудования и аппаратных платформ для развертывания приложений.

Существует необходимость выявления опасности нежелательных последствий или потенциально возможного ущерба для организации в результате использования ею облачной среды. Решение этой проблемы связано с проведением анализа рисков и разработкой метода численной оценки риска нарушения информационной безопасности (ИБ) в системе облачных вычислений (СОбВ). В данной работе СОбВ названа информационная система, в которой взаимодействуют заказчик услуг и вендор.

Известно, что невозможно оценить риск нарушения информационной безопасности в общем виде [2]. Поэтому, для анализа рисков в работе предложен возможный вариант архитектуры СОбВ, представленный на рисунке 1. На рисунке 1: R – маршрутизатор, F – межсетевой экран, AN – антивирус, OS – операционная система, App – приложение, web – web-сервер, Blade – Blade-сервер, FTP – файловый сервер, DNS – DNS-сервер. Кластеры серверов работают в виртуальной среде.

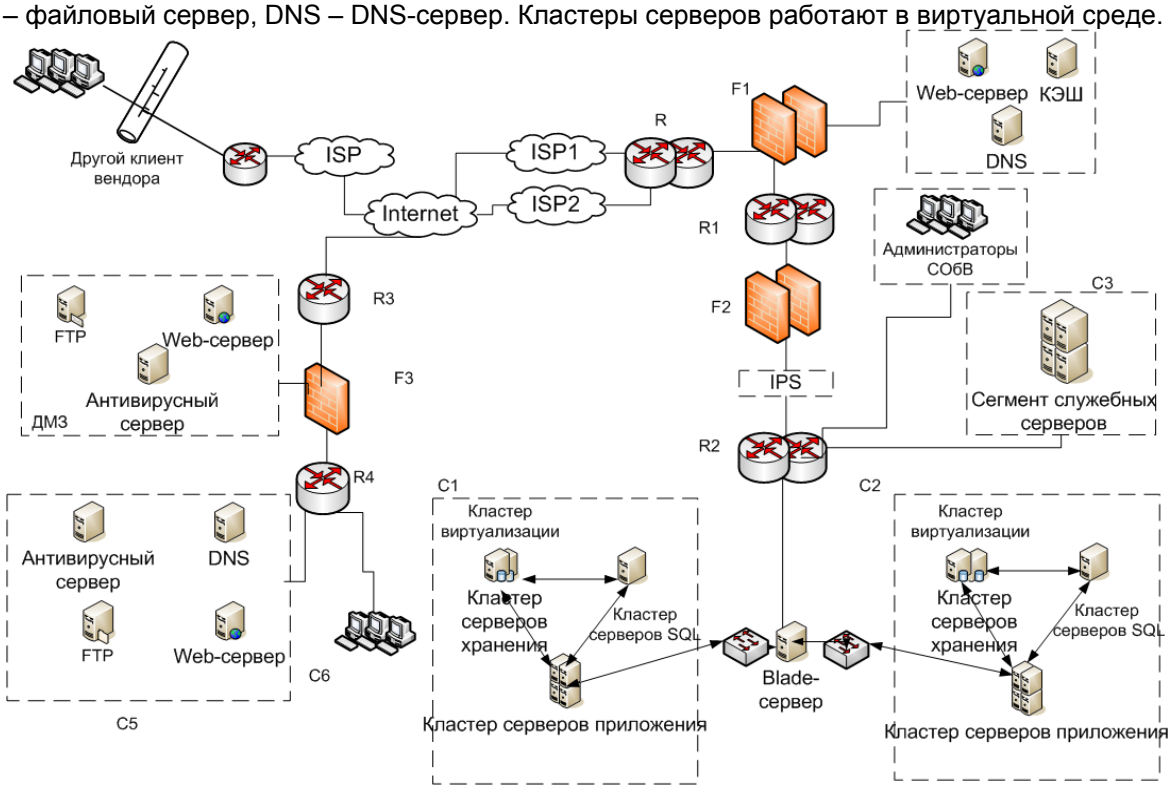


Рис. 1. Вариант архитектуры системы облачных вычислений

Анализ рисков представляет собой процесс выявления зависимости между значением риска нарушения информационной безопасности и параметрами, от которых он зависит. В процессе анализа рисков должны быть идентифицированы угрозы, источники угроз, уязвимости, а также проведена оценка средств защиты и мер противодействия.

Метод расчета прогнозируемого риска нарушения информационной безопасности, основанный на построении нечетких когнитивных карт (НКК), был предложен и описан в [3]. В данной работе этот метод применен к новому объекту защиты − системе облачных вычислений. В работе представлены результаты разработки модели угроз в СОбВ в виде нечетких когнитивных карт. Нечеткие когнитивные карты были разработаны с учетом всех возможных источников угроз и компонентов инфраструктуры СОбВ, расположенных на путях распространения атак. Метод позволяет получить оценку прогнозируемого значения уровня риска нарушения информационной безопасности для наихудшего случая, когда одновременно активизируются все возможные источники угроз.

Метод применим на стадии проектирования системы обеспечения информационной безопасности СОбВ. Он позволяет проектировщику оценить вклад в значение уровня риска угроз, реализуемых злоумышленником, внутренним пользователем заказчика, другим клиентом вендора, администратором вендора в СОбВ.

Одна из нечетких когнитивных карт, составляющих модель угроз в СОбВ, представлена на рисунке 2. На рисунке 2 источники угроз обозначены: $S^{внш_кл}$ - другой клиент вендора и запущенные им несанкционированные процессы; $S^{зл}$ - злоумышленник – несанкционированный субъект доступа и запущенные им процессы. Объекты атак обозначены: O_{C1} и O_{C2} – защищаемые информационные ресурсы основного и резервного кластера виртуализации; O_{C3} – информационные ресурсы в серверном сегменте вендора; O_{C4} – информационные ресурсы КЭШ-сервера; O_{C5} – информационные ресурсы в серверном сегменте на стороне компании заказчика; W() - значения уровней уязвимостей.

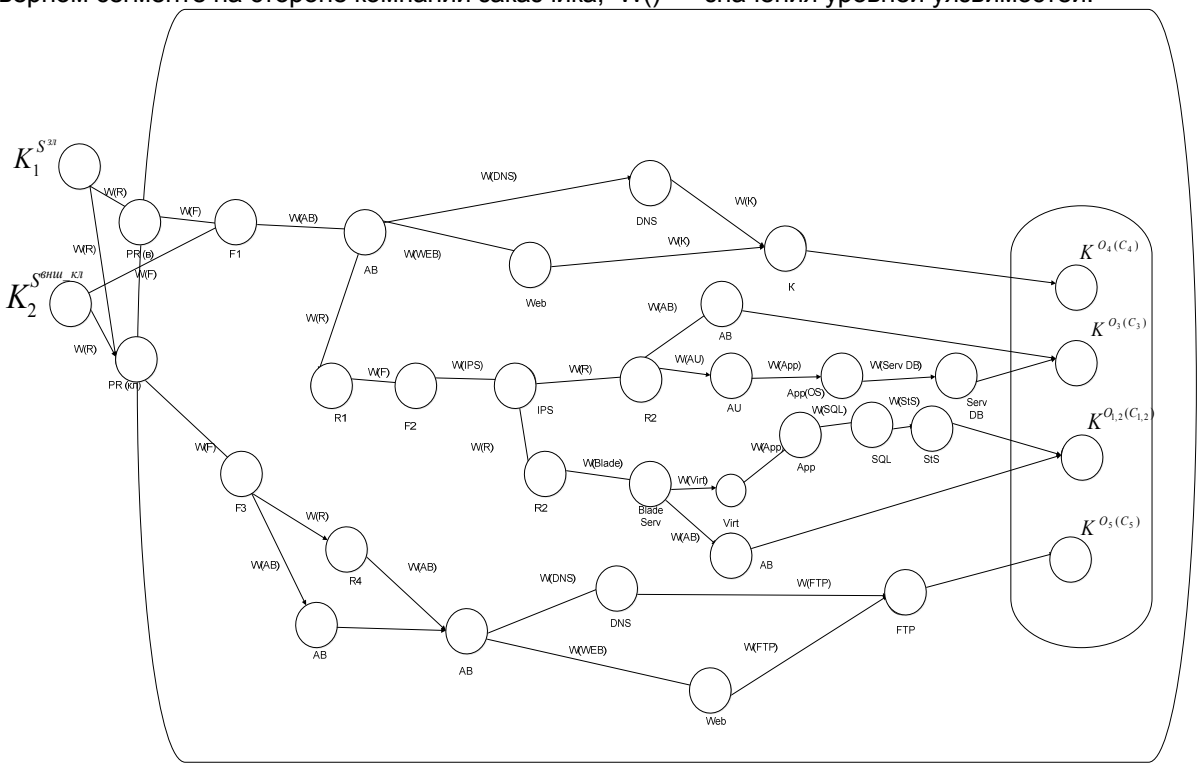


Рис. 2. Модель внешних угроз несанкционированного доступа в СОБВ

Результаты расчетов прогнозируемого значения риска нарушения информационной безопасности представлены в таблице 1.

В таблице 1 значения вероятностей угроз, реализуемых: $P^{зл}$ - злоумышленником; $P^{внш_кл}$ - другим клиентом вендора; $P^{адм}$ - сотрудником или администратором вендора; $P^{вн}$ - внутренним сотрудником заказчика (нарушителем политики безопасности); $P_{утеч}$ - вероятность угрозы утечки.

Эти результаты показали применимость предложенного метода для СОбВ. При проектировании системы обеспечения ИБ или в процессе планирования полученные результаты позволяют определить, в какой степени может быть достигнута поставленная цель защиты.

Кроме того, полученные результаты могут быть использованы для численной оценки риска нарушения ИБ в реальном масштабе времени, когда детектируются некоторые опасные события в информационной среде СОбВ.

Таблица 1

Расчет прогнозируемых значений риска нарушения ИБ на основе построения НКК

Сегм	Цен	Pu_зл	Pu_внш_кл	Pu_адм	Pu_вн	Pu_утеч	Рез уровень угроз	Уровень рискаRo
C1	0,4	0,07	0,019	0,15	0,02	0,2	0,19	0,075
C2	0,4	0,07	0,019	0,15	0,02	0,2	0,19	0,075
C3	0,06	0,05	0,12	0,4	0,1	0,4	0,42	0,025
C4	0,04	0,07	0,46	0,18	0,6	0,08	0,5	0,02
C5	0,1	0,22	0,28	0,057	0,5	0,4	0,47	0,047
								0,24

Оценивание риска нарушения ИБ в реальном масштабе времени необходимо для принятия оперативных решений по реагированию на инциденты. При этом должна использоваться автоматизированная система, содержащая базу знаний, применим механизм искусственной нейронной сети (ИНС).

Сегодня главной проблемой использования искусственной нейронной сети является формирование множества данных обучающей выборки, достаточной для обучения ИНС. Используя результаты прогнозируемых значений рисков нарушения информационной безопасности, рассчитанных для СОбВ, можно сформировать массив данных обучающей выборки для настройки ИНС. Фрагмент экспериментального массива данных для обучения нейронной сети представлен в таблице 2.

В таблице №2 Pa – вероятность активизации угрозы по тому или иному пути. При настройке ИНС переменная принимает значения в диапазоне [0,1] с шагом дискретизации 0,1. Если атака будет зафиксирована на одном из путей, то Pa принимает значение 1.0 на этом пути.

Риск нарушения информационной безопасности в случае, когда все возможные источники угроз активизируются одновременно, обозначен как $R_{\Sigma}(P_a)$. В случае, когда активизируется только один из источников угроз, риск нарушения информационной безопасности обозначается: R_{ad}, если источник угрозы - злоумышленник, R_{cu}, если источник угрозы другой клиент вендора, R_{lu}, если источник угрозы сотрудник заказчика, R_{av}, если источник угрозы сотрудник или администратор вендора.

Следует также отметить, что для формирования обучающей выборки, достаточной для обучения нейронной сети, в качестве входных данных ИНС были выбраны также значения ценностей информационных активов (V_a). Таким образом, множество данных обучающей выборки должно включать следующие факторы: P_a V_a.

Таблица 2

Фрагмент экспериментального массива данных для обучения ИНС

	Атака на все сегменты СОбВ					Атака на сегмент 1 (класт. вирт.)				
Pa	Сумм	ЗЛ	ВНШ_КЛ	АДМ_В	ВН_КЛ	Сумм	ЗЛ	ВНШ_КЛ	АДМ_В	ВН_КЛ
0	0	0	0	0	0	0	0	0	0	0
0,1	0,073	0,86	0,0069	0,0305	0,0292	0,0179	0,0029	0,0008	0,0121	0,0023
0,2	0,1385	0,01	0,0137	0,604	0,0555	0,0352	0,0058	0,0015	0,024	0,0047
0,3	0,1976	0,02	0,0206	0,0898	0,0792	0,0518	0,0087	0,0023	0,0357	0,007
0,4	0,251	0,03	0,0275	0,1185	0,1004	0,068	0,0116	0,003	0,0473	0,0093
0,5	0,2995	0,04	0,0344	0,1467	0,1194	0,0835	0,0145	0,0038	0,0586	0,0116
0,6	0,3436	0,05	0,0412	0,1743	0,1364	0,0985	0,0174	0,0045	0,0698	0,0139
0,7	0,384	0,06	0,0418	0,2014	0,1516	0,113	0,0203	0,0053	0,0808	0,0162

0,8	0,4211	0,06	0,55	0,2279	0,1652	0,127	0,0232	0,006	0,0916	0,0184
0,9	0,4553	0,07	0,0618	0,2538	0,1773	0,1405	0,0261	0,0068	0,1022	0,0207
1	0,487	0,08	0,0687	0,2791	0,1881	0,1534	0,029	0,0075	0,1126	0,023

Искусственная нейронная сеть может быть использована для расчета оперативного значения уровня риска нарушения информационной безопасности, связанного с появлением угрозы в реальном масштабе времени. Схема реализации метода проиллюстрирована на рисунке 3.

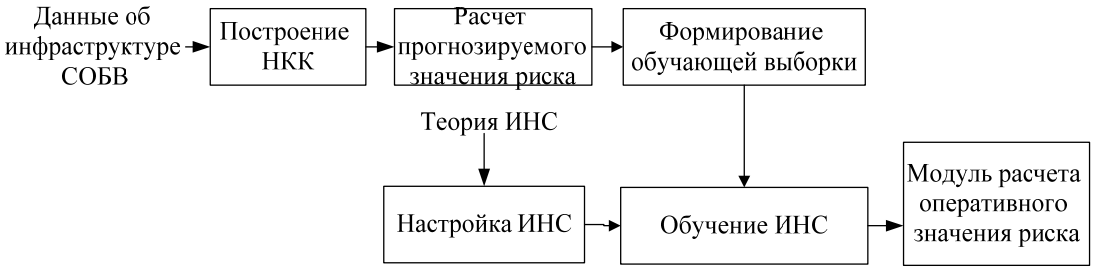


Рис. 3. Схема реализации метода расчета оперативного значения риска нарушения информационной безопасности

Для обучения ИНС с помощью сформированного массива данных был использован программный модуль Matlab 6.0. В процессе настройки нейронной сети выбран однослойный персептрон с числом нейронов в скрытом слое, равным двадцати. Нейронная сеть прошла 33 эпохи, постепенно обучаясь и сокращая ошибку обучения. В конце эксперимента ошибка была равна 10^{-6} мсэ.

Предлагаемые решения на основе НКК и ИНС могут быть применимы специалистами в области информационной безопасности для управления рисками нарушения ИБ в СОбВ − уменьшения значения уровня риска до приемлемого уровня за счет выбора рационального варианта реагирования на атаку в реальном масштабе времени.

СПИСОК ЛИТЕРАТУРЫ

1. Н. Антонопулус, Л. Джиллиам Облачные вычисления: Принципы, системы, применение. — изд-во Спрингер, 2010. — 379 с.
2. С.С. Корт Теоретические основы защиты информации: учебное пособие для вузов по группе специальностей в области информационной безопасности – Изд-во «ПИТЕР», 2004. – 240 с.
3. М.Б. Гузаиров, И.В. Машкина, Е.С. Степанова М. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности. – Журнал «Безопасность информационных технологий» №2, 2011. С. 37-49.

УДК 004.056

РАССЧЕТ ИНФОРМАТИВНОСТИ ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ, ОСНОВАННОГО НА КОРТЕЖЕ ЛИНГВИСТИЧЕСКИХ ПРИЗНАКОВ

Сухопаров М.Е.,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверский пр., д. 49,
e-mail: sukhoparovm@gmail.com

Аннотация. Одним из направлений развития теории информационной безопасности является разработка моделей, методов идентификации и аутентификации пользователей порталов сети Интернет. Целью работы является оценка информативности лингвистических признаков текстовых сообщений, позволяющих создавать авторский профиль для обнаружения лиц, пишущих комментарии под несколькими учетными записями. Приведены особенности текстовых сообщений, предложена модель сообщения. Проведен эксперимент, показывающий возможности использования адаптированного анализатора для вычисления синтаксических паттернов и структур. Определена структура профиля пользователя для процессов идентификации и аутентификации порталов сети Интернет. Оценена информативность признаков с помощью подхода на основе энтропии Шеннона.

Ключевые слова: *оценка информативности, лингвистический профиль, энтропия Шеннона.*

EVALUATION OF INFORMATIVE OF LINGUISTIC USER PROFILE

Sukhoparov M.E.,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: sukhoparovm@gmail.com

Abstract: One of the directions of development of the theory of information security is to develop models, methods of identification and authentication of users of the Internet portals. The aim of the work is to evaluate the informativeness of linguistic features of text messages, allowing you to capture the author's profile for face detection, when posting under multiple accounts. Are the features of text messages, we propose a model of the message. An experiment showing the possibilities of using the analyzer adapted to compute syntactic patterns and structures. The structure of the user profile for the identification and authentication portal on the Internet. Estimated informative features using an approach based on the Shannon entropy.

Keywords: *evaluation of information content, linguistic profile, Shannon entropy.*

Введение. Появление специализированных сервисов, обеспечивающих обмен мнениями между посетителями порталов и сайтов сети Интернет, акцентирование большого внимания тональностям комментариев и сообщений рядовых пользователей вызывает необходимость разработки специализированных систем мониторинга информационной безопасности [1].

Одной из задач подобных систем является обнаружение различных проявлений манипуляции и искусственного формирования общественного мнения, путем «организации» целенаправленных тематических диалогов, в которых ряд пользователей имеют несколько учетных записей [2].

В связи с этим возникает задача совершенствования методического аппарата определения авторства, верификации авторов текстов, коротких сообщений различных порталов сети Интернет.

Постановка задачи в общем случае задачу можно сформулировать следующим образом. Имеется текст неизвестного автора, набор возможных авторов сообщений портала сети Интернет, для каждого автора есть примеры текстов. Необходимо определить на основе анализа сообщений пользователя, имеющего одну учетную запись, могут ли они также принадлежать автору, зарегистрированному под другой учетной записью. Т.е. на основе лингвистических признаков выявить авторов, оставляющих комментарии под разными учетными записями.

В данном случае под текстом понимается совокупность предложений и конструкций с использованием естественного русского языка, составляющих короткие сообщения и комментарии пользователей порталов сети Интернет [3], [4], [5].

Текстовые сообщения открытых порталов сети Интернет имеют ряд особенностей:

– умышленное искажение словоформ русского языка, затрудняющее автоматическую обработку сообщений;

– грамматически неправильно построенные фразы;

– использование специфической лексики, аббревиатур и конструкций, характерных для целевой аудитории ресурса ИТКС;

– небольшое количество слов в сообщениях;

– повсеместное отсутствие орфографической, пунктуационной, грамматической и стилистической коррекции.

Один из основных вопросов состоит в том, какие свойства использовать для классификации.

Исследования в области определения авторства текста позволяют выделить ряд классов признаков: символьные, лексические, синтаксические, семантические, тематические [6], [7], [8]. В ряде работ по идентификации принадлежности текстов, синтаксическая информация считается более надежной по сравнению с лексической при определении автора.

Предлагаемый метод Особенности коротких сообщений накладывают ряд своих ограничений, приводящих к необходимости использования целого спектра признаков как лингвистического, так и статистического. Однако при «внешнем» анализе комментариев, ряд статистических признаков (cookie, время сетевой активности, периодичность сессии) может быть недоступен. Исходя из этого особую актуальность приобретают лингвистические признаки.

Большое количество исследователей [9], [10] отмечают, что авторы, как правило, бессознательно используют синтаксические структуры, в связи с чем, возникает необходимость их обработки и анализа предоставляемого ими признакового пространства. Таким образом, одним из направлений является поиск синтаксических паттернов в комментариях и коротких текстов блогов и порталов сети Интернет.

Ввиду особенностей обрабатываемой информации для автоматической обработки текстов был использован модифицированный анализатор на базе словаря В.А. Тузова [11].

С целью уменьшения числа нераспознанных конструкций, возникающих вследствие большого количества орфографических, стилистических, синтаксических и других ошибок, для достижения приемлемого уровня распознавания морфосинтаксической информации словарная база данных была дополнена информацией о специфических выражениях, символах.

Кроме того, был применен эвристический метод определения морфологической информации неизвестной словоформы, основанный на продукционных правилах, учитывающих морфологические описатели окружения словоформы и совпадение в базе данных окончаний [12], что позволило строить последовательности синтаксических конструкций комментариев.

Использование возможностей модифицируемой версии синтаксического анализатора, позволяет в упрощенном виде представить модель сообщения пользователя в следующим виде:

$$M =< L, SS, SLP, SP, SE, H > \quad (1)$$

L – лексический словарь, содержит слова и их частоты, употребляемые комментатором портала.

SLP – база данных шаблонов буквенных сокращений и символьно-буквенных сочетаний.

SS – графематическая база данных, в которой находятся данные о знаках препинания, их употреблении в сообщениях, а также специальные символы.

SP – синтаксическая база данных, включающая информацию о шаблонах (синтаксических паттернах).

SE – специальные выражения, характерные для форума и употребляемые пользователем в своих комментариях.

H – шум или нераспознанные словоформы.

На рисунке 1 приведены результаты работы анализатора, полученные при обработке форума, посвященного обсуждению ряда автомобильных тематик.

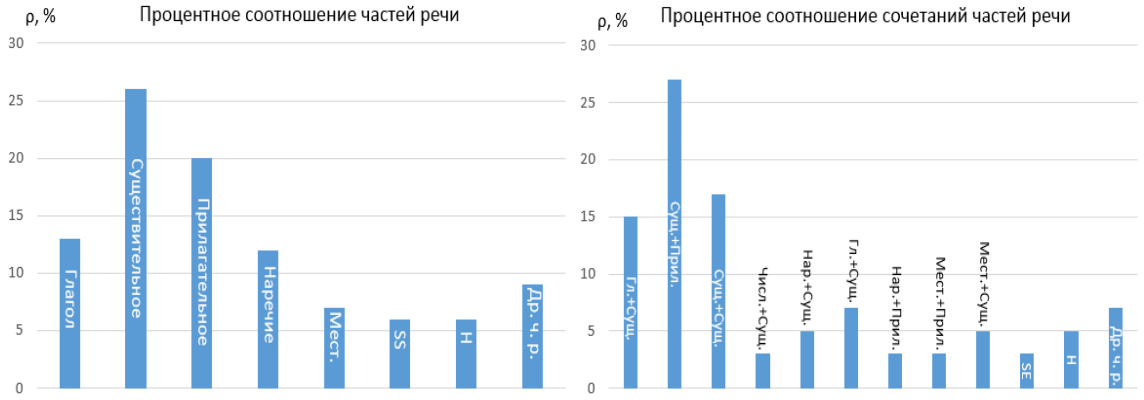


Рис.1. Результаты вычисления морфологической информации частей речи и их сочетаний

Особенностью данного подхода являлось использование «шумовых» нераспознанных словоформ H.

Модель сообщения дает возможность определить структуру профиля пользователя для процессов идентификации и аутентификации порталов сети Интернет. Процентное соотношение перечисленных в (1) характеристик на рисунке 2 дает наглядное представление о различиях «авторского» стиля комментаторов.

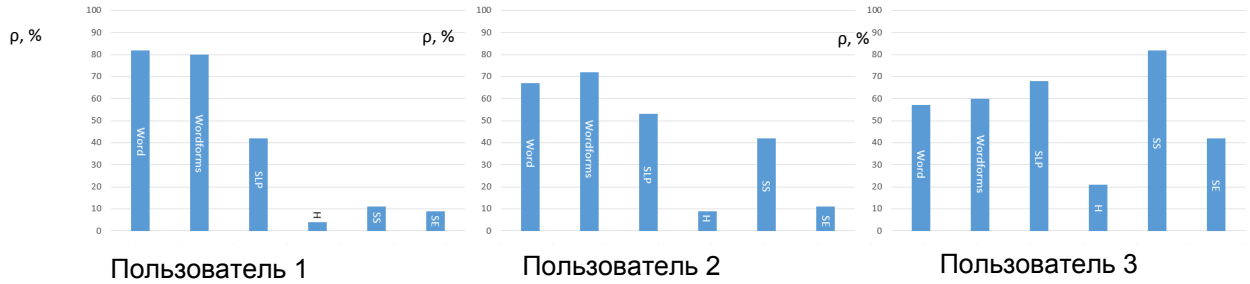


Рис.2. Результаты вычисления морфологической информации частей речи и их сочетаний

С целью оптимального использования характеристик модели сообщения возникает вопрос определения наиболее информативных признаков. Оценка информативности производилась с помощью подхода на основе энтропии Шеннона, где в качестве признаков использовались синтаксические структуры, пример которых представлен в таблице 1.

$$I(x_i) = 1 + \left(\sum_{i=1}^{G} P_i \sum_{k=1}^{K} P_{i,k} \log_K P_{i,k} \right), \quad (2)$$

где G – количество градаций признака;

K – количество классов;

P_i^o – вероятность i-той градации признака.

$$P_i = \frac{\sum_{k=1}^{K} m_{i,k}}{N}, \qquad (3)$$

где $m^o_{i,k}$ – частота появления i-той градации в K-том классе;

N – общее число наблюдений.

P_{i,k^o} – вероятность появления i-той градации признака в K-том классе.

$$P_{i,k} = \frac{m_{i,k}}{\sum_{k=1}^{K} m_{i,k}}. \qquad (4)$$

Таблица.1.

Оценка информативности синтаксических признаков

Обозначение	Описание	$I(x_i)$	$I'(x_i)$
S + Pril	Существительное + прилагательное	0,67	0,6
S + G	Существительное + глагол	0,58	0,52
S + S	Существительное + существительное	0,5	0,46
Ch + S	Числительное + существительное	0,4	0,36
Nar + S	Наречие + существительное	0,42	0,41
Nar + Pril	Наречие + прилагательное	0,4	0,38
G + Nar	Глагол + Наречие	0,45	0,4
G + S	Глагол + существительное	0,46	0,43
Mest+Pril	Местоимение + прилагательное	0,41	0,39
Mest+S	Местоимение + существительное	0,45	0,42
G + Predl + S	Глагол + предлог + существительное	0,48	0,41
Predl + S + S	Предлог + существительное + существительное	0,34	0,3
S + Predl + S	Существительное + предлог + существительное	0,52	0,46
S + G + Nar	Существительное + глагол + наречие	0,43	0,39
S + S + SS	Существительное + существительное + специальный символ	0,56	0,51
G + S + SS	Глагол + существительное + специальный символ	0,57	0,52
S + Predl + Pril	Существительное + предлог + прилагательное	0,31	0,27
S + Nar + Pril	Существительное + наречие + прилагательное	0,34	0,3

На основании проведенной выборки были получены результаты, представленные на рисунке 3.

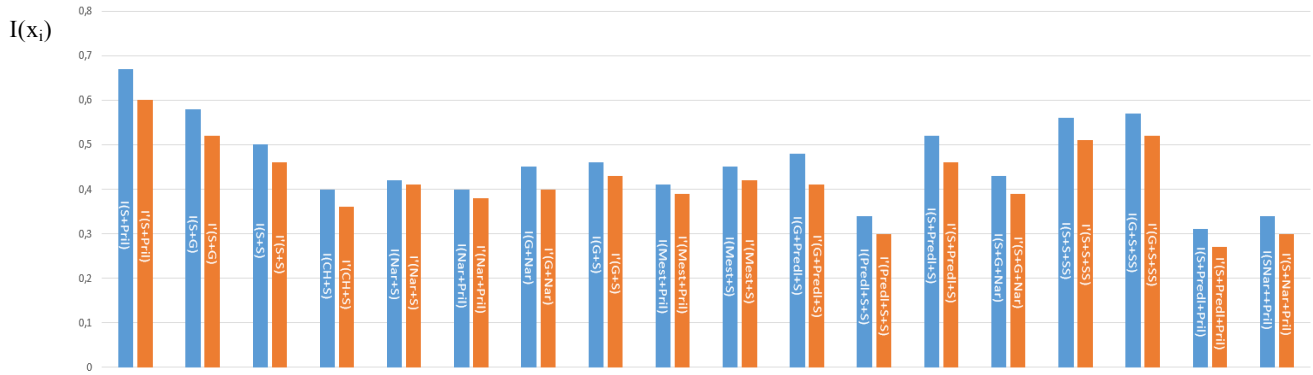


Рис.3. Информативность синтаксических структур

Заключение. Использование синтаксического анализатора позволяет увеличить количество характеристик лингвистического признакового пространства для идентификации авторства текстов. Каждый признак обладает своей информативностью.

Нераспознанные словоформы, возникающие в результате опечаток и орфографических, стилистических, пунктуационных ошибок, несовершенства анализатора, также могут являться характеристикой автора комментария портала сети Интернет.

Вследствие несовершенства синтаксических анализаторов данные могут быть зашумлены, поэтому, в идеале, необходимо использовать несколько различных признаковых пространств, включающих в себя частотные распределения частей речи, локальный синтаксис, глобальную структуру предложения, словосочетания определенного типа.

СПИСОК ЛИТЕРАТУРЫ

1. He Q., Glas C.A.W., Kosinski M., Stillwell D.J., Veldkamp B.P. Predicting self-monitoring skills using textual posts on Facebook Source of the Document Computers in Human Behavior (33) 2014, pp 69-78.
2. Гвоздев А.В., Лебедев И.С., Зикратов И.А. Вероятностная модель оценки информационного воздействия. //Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 99-103.
3. Лебедев И.С., Сухопаров М.Е. Методика идентификации авторства текстов на основе методов математической лингвистики. //В мире научных открытий. 2014. № 6.1 (54). С. 599-622.
4. Тузов В.А. Компьютерная семантика русского языка. – СПб.: Изд-во СПбГУ,2004. – 400 с.
5. Боярский К.К., Каневский Е.А. Разработка инструментария для полуавтоматической морфологической разметки текста // Труды международной конференции «Корпусная лингвистика – 2008». – СПб.: С-Петербургский гос. Университет, Факультет филологии и искусств, 2008. С. 83 – 88.
6. Т.В.Батура Формальные методы определения авторства текстов.// Вестник НГУ. Серия: Информационные технологии. Т.10, № 4, 2012 С.81-94.
7. Khmelev D.V., Teahan W.J. (2003a). A repetition based measure for verification of text collections and for text categorization. In Proceedings of the 26th ACM SIGIR (pp. 104–110). NewYork: ACM Press.
8. Хмелёв Д.В. Распознавание автора текста с использованием цепей А.А. Маркова//Вестник МГУ. Сер. 9, Филология. 2000. № 02. С.115-126.
9. Karlgren J., & Eriksson G. (2007). Authors, genre, and linguistic convention. In Proceedings of the SIGIRWorkshop on Plagiarism Analysis, Authorship Attribution, and Near-Duplicate Detection (pp. 23–28).
10. Rytter W. Application of Lempel-Ziv factorization to the approximation of grammar-based compression Theoretical Computer Science,2003, 302 (1-3), pp. 211-222.
11. Тузов В.А. Компьютерная семантика русского языка. – СПб.: Изд-во СПбГУ,2004. – 400 с.
12. Лапшин С.В., Лебедев И.С. Метод полуавтоматического формирования словаря морфологических описаний слов. //Научно-технический вестник информационных технологий, механики и оптики. 2012. № 5 (81). С. 106-110.

УДК 004.056.5

ЗАЩИТА РЕСУРСОВ ГИС

Татарникова Татьяна Михайловна[1] Яготинцева Наталья Владимировна[2],
[1] Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
[2] Российский государственный гидрометеорологический университет,
Россия, Санкт-Петербург, Малоохтинский пр., д. 98,
e-mail: tm-tatarn@yandex.ru.

Аннотация: Приводится структурно-функциональная модель ГИС, из которой определены элементы, подверженные угрозам информационной безопасности. Перечислены наиболее характерные виды угроз для ГИС. Выполнена постановка задачи синтеза системы защиты информации в ГИС и раскрыты этапы ее решения.

Ключевые слова: *информационная безопасность; угроза; система защиты информации; вероятность угрозы; комплексное решение.*

RESOURCE PROTECTION GIS

Tatarnikova Tatiana [1], Yagotinceva Natalia [2],
[1] Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2] Russian State Hydrometeorological University,
Russia, St. Petersburg, Malookhtinsky prospect, 98,
e-mail: tm-tatarn@yandex.ru.

Abstract: Provides structural and functional model of GIS, which sets out the elements at risk for information security. Are the most typical types of threats for a GIS. Formulation of the problem is made of synthesis of information security in the GIS and disclosed the steps of the solution.

Keywords: *information security; threat; security system; the probability of threats; comprehensive solution.*

Введение. Обеспечение информационной безопасности ГИС, как и для любой неоднородной сложной информационной системы, решается с применением комплексного подхода, который в соответствии с общей концепцией информационной безопасности включает вопросы конфиденциальности, доступности и целостности информации [1].

Для различных ГИС, решающих определенные задачи требуется соответствующая стратегия по защите данных. В ситуации, когда ГИС используется для решения корпоративных задач, карты и их содержание обладают коммерческой ценностью.

Поэтому необходимо обеспечить как конфиденциальность хранимой и передаваемой информации, так и разграничение доступа к ней.

В ситуации же, когда используется ГИС массового использования, больший упор должен быть сделан в сторону защиты информации от повторного использования.

В свою очередь, стоит обратить внимание, что при организации защиты ГИС государственного значения помимо разработки технических и программных средств согласно требованиям федеральной службы по техническому и экспортному контролю необходима сертификация систем и средств защиты информации и аттестацию объектов информатизации по требованиям безопасности [2], [3].

1. Структурно-функциональные элементы ГИС, подверженные угрозам информационной безопасности.

ГИС, как систему в целом, можно разделить на несколько структурно-функциональных элементов, среди которых выделим следующие [4]:

– автоматизированное рабочее место пользователя (АРМ), которое включает в себя системное и прикладное программное обеспечение (ПО), а именно: средства хранения, ввода и вывода информации;

– сетевой сервер, содержащий специализированное программное обеспечение, используемое для хранения данных ГИС. Сервер содержит средства хранения, ввода и вывода информации, а также системное и прикладное ПО. Помимо перечисленного неотъемлемой частью является система управления базами данных (СУБД).

– телекоммуникационная система, обеспечивающая передачу информации по каналам связи (Internet, выделенные каналы). Составляющими, снабженными специальным программным обеспечением, являются модем и маршрутизатор, который пересылает пакеты данных между различными сегментами сети, и в случае необходимости принимает решения о пересылке.

Также в состав ГИС помимо АРМ пользователя входят и иные служебные рабочие места. Речь идет о программистах, техническом персонале, администраторе сети и администраторе безопасности – все они важны при организации любой значительной структуры ГИС.

Ниже на рис. 1 схематически отображена модель ГИС.

Во время информационного взаимодействия структурно-функциональных элементов ГИС между собой и с внешней средой возникает вероятность возникновения угрозы. Наиболее характерными видами угроз для ГИС являются [5]:

– кража информации и носителей информации, несанкционированное копирование. Данный вид угроз возникает на этапах первоначального сбора информации средствами ввода, получение доступа к которым и является причиной возникновения угрозы.

– перехват информации по линиям электропитания и по посторонним проводникам за счет побочного электромагнитного излучения или по акустическому каналу. Такие угрозы возникают во время доставки или обмена информацией между различными АРМами и сервером с применением телекоммуникационной системы.

– подмена данных. Данный вид угроз возможен на этапе вывода информации при получении злоумышленником несанкционированного доступа вследствие слабой системы аутентификации и идентификации, в том числе разграничения прав доступа.

– уничтожение программного обеспечения, данных ГИС, файлов, в том числе паролей и ключевой информации. Данному виду угроз подвержены средства хранения информации.

– ошибки при установке различного программного обеспечения (ПО), операционной системы и базы данных, а так же при написании и эксплуатации ПО. Угрозы этого вида характерны для сервера ГИС при получении несанкционированного доступа к нему.

– подмена или модификация операционных систем, систем управления базами данных, прикладных программ, различных данных, ключевой информации и правил доступа. Такой вид угроз направлен на сервер ГИС.

– нарушение правил доступа, иными словами, взлом. Угроза направлена на сервер ГИС после успешной реализации предыдущей угрозы.

– уменьшение скорости обработки информации, пропускной способности каналов связи, объемов свободной оперативной памяти и дискового пространства, нарушение электропитания. Эта угроза является некоторым следствием реализации выше перечисленных угроз.

Таким образом, широкий спектр угроз для безопасности ГИС говорит о необходимости использования комплекса защитных мер по обеспечению безопасности данных в ГИС.

2. Комплекс защитных мер по обеспечению безопасности данных в ГИС.

Согласно ГОСТ Р ИСО/МЭК 17799-2005 информационная безопасность в информационных системах в целом сводится к защите конфиденциальности, целостности и доступности.

Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. Другими словами каждый пользователь должен получать доступ только к информации, для которой у него есть необходимые права.

Целостность: обеспечение достоверности и полноты информации и методов ее обработки. Иными словами данные не должны быть изменены при их хранении, передачи или представлении.

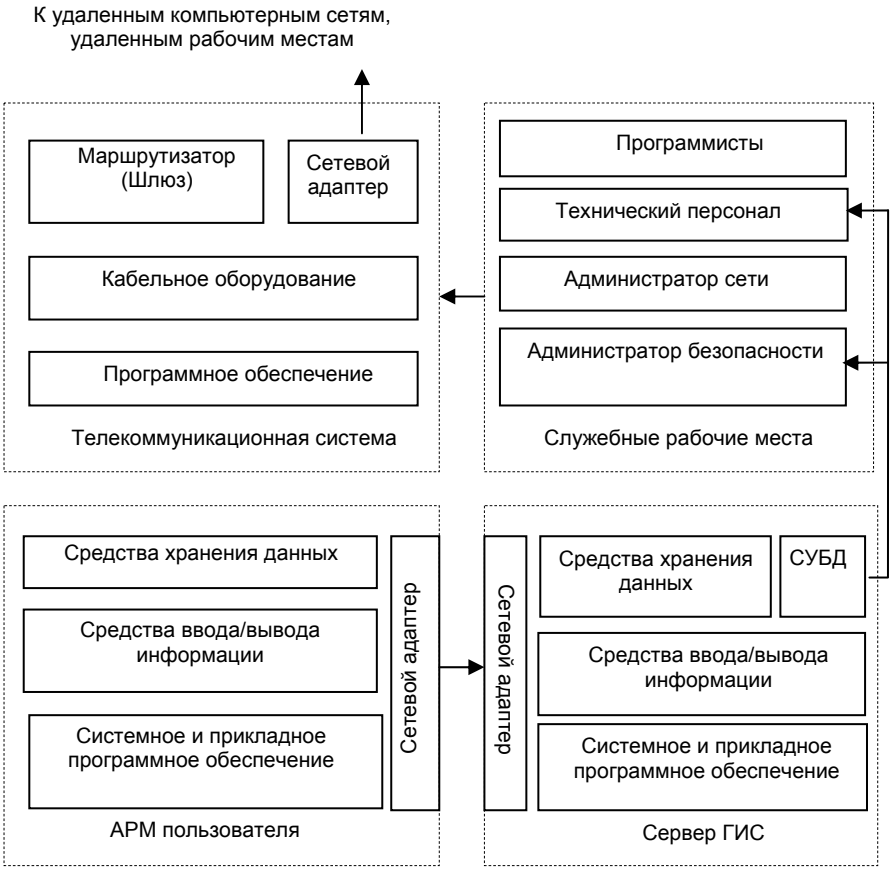


Рис. 1. Структурно-функциональная модель ГИС

Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости. Иными словами беспрепятственная реализация прав доступа субъектами, авторизованных в системе, к информации в соответствии с политикой доступа.

Конфиденциальность в ГИС решается криптографическими методами, среди которых важное место занимает шифрование. К примеру, при использовании мобильного приложения ArcGis, пользователям ГИС предоставляется возможность применить шифрование КЭШ-памяти своего мобильного устройства. Для приложений ArcPad применяется шифрование файла данных и карт памяти. В ГИС «Панорама» встроены средства шифрования пространственных данных 256-битным ключом при отправке и получении, что предотвращает перехват или подмену данных в процессе передачи. Отметим, что применение шифрования уменьшает скорость передачи данных – время задержки составляет от 3 до 10 процентов от общего времени.

Другой способ обеспечения конфиденциальности данных – это предоставление доступа только авторизованным пользователям (субъектам доступа), который решается через задачу разграничения доступа. Субъектом доступа называется лицо или процесс, действия которого регламентируются правилами разграничения доступа. В ГИС субъектом доступа могут быть сотрудники, которые наделены уникальными идентификаторами, и которые являются пользователями сети. Сетевые потоки, которые обеспечивают связь между сотрудником и сервером ГИС, или сетевые потоки, которые являются запросами к базе данных ГИС, также являются субъектами доступа.

Методы разграничение доступа (в основном по паролю) широко распространен в ГИС от КБ «Панорама», программах компании ESRI – ArcGis, ArcSDE, в службах Oracle Advanded Security и СУБД Oracle.

3. Постановка задачи синтеза системы защиты информации в ГИС.

Пусть информация ГИС подвержена некоторой совокупности угроз со стороны злоумышленника. Каждая угроза характеризуется вероятностью появления и наносимым ущербом. Уменьшение общего ущерба, наносимого ГИС обеспечивается применением системы защиты информации (СЗИ) [6].

Введем следующие обозначения:

Pi – вероятность появления i-й угрозы, $i = \overline{1, n}$;

qi – ущерб, наносимый i-й угрозой;

$\overline{W}$ – общий предотвращенный ущерб ГИС;

$\overline{w}_i$ – предотвращенный ущерб за счет ликвидации воздействия i-й угрозы;

$P_i^{\text{устр}}$ – вероятностью устранения каждой i-й угрозы;

Тогда, задачу синтеза системы защиты информации в ГИС в общем виде сформулируем следующим образом: выбрать вариант реализации СЗИ, обеспечивающий максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на СЗИ [3].

Формальная постановка задачи примет вид: найти

$$T^{\text{доп}} = \max \overline{W}(T),\ T^{\text{опт}} \in T^{\text{доп}} \tag{1}$$

при ограничении

$$C = \left(T^{\text{доп}}\right) \le C_{\text{доп}}), \tag{2}$$

где *C* – вектор стоимости аппаратной реализации СЗИ;

T – вектор, характеризующий вариант аппаратной реализации СЗИ

$T^{\text{доп}}$, $T^{\text{опт}}$ – допустимое и оптимальное значение вектора *T*;

$C_{\text{доп}}$ – допустимые затраты на СЗИ.

Для решения задачи необходимо сформировать показатель качества функционирования системы защиты информации $\overline{W}(T)$.

Тогда, предотвращенный ущерб в общем виде выражается соотношением:

$$\overline{W} = F\left(P_i, q_i, P_i^{\text{устр}}\right), i = \overline{1,n}. \tag{3}$$

Предотвращенный ущерб за счет ликвидации воздействия *i*-й угрозы

$$\overline{w}_i = P_i \cdot q_i \cdot P_i^{\text{устр}},\ \ i = \overline{1,n}. \tag{4}$$

При условии независимости угроз и аддитивности их последствий получаем

$$\overline{W} = \sum_{i=1}^{n} P_i \cdot q_i \cdot P_i^{\text{устр}}. \tag{5}$$

Вероятность появления *i*-й угрозы P_i определяется статистически и соответствует относительной частоте ее появления

$$P_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}, \tag{6}$$

где λ_i – частота появления *i*-й угрозы.

Ущерб q_i, приносимый *i*-й угрозой может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или «испорченной» информации и т.д. Однако, на практике оценить ущерб затруднительно, особенно на ранних этапах проектирования СЗИ. Целесообразно вместо абсолютной оценки ущерба использовать относительную, который представляет собой степень опасности *i*-й угрозы для ГИС. Степень опасности может быть определена экспертным путем в предположении, что все угрозы для ГИС составляют полную группу событий, то есть

$$0 \le q_i \le 1,\ \sum_{i=1}^{n} q_i = 1.$$

Наиболее сложным вопросом является определение вероятности устранения *i*-й угрозы $P_i^{\text{устр}}$ при проектировании СЗИ. Примем допущение о том, что эта вероятность определяется тем, насколько полно учтены качественные и количественные требования к СЗИ при их проектировании, то есть

$$P_i^{\text{устр}} = f_i\left(x_{i1}, ..., x_{ij}, ..., x_{im}\right), \tag{7}$$

где x_{ij} – степень выполнения *j*-го требования к СЗИ для устранения *i*-й угрозы, $i = \overline{1,n};\ \ j = \overline{1,m}$.

Пусть первые *k* требований будут количественными $\left(j = \overline{1,k}\right)$ остальные (*m*-*k*) – качественными $\left(j = \overline{k+1,m}\right)$.

Степень выполнения *j*-го количественного требования определяется его близостью к требуемому (оптимальному) значению.

Для оценки степени выполнения *j*-го количественного требования к СЗИ удобнее всего использовать его нормированное значение $\overline{x}_{ij}\left(j = \overline{1,k}\right),\ \ 0 \le x_{ij} < 1$.

Для нормирования удобно использовать функцию вида

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij}^{\text{НХ}}}{x_{ij}^{\text{НЛ}} - x_{ij}^{\text{НХ}}}, \tag{8}$$

где x_{ij} – текущее значение *j*-го требования;

$x_{ij}^{\text{НЛ}}$, $x_{ij}^{\text{НХ}}$ – наилучшее и наихудшее значения.

Степень выполнения *j*-го качественного требования определяется функцией принадлежности к наилучшему значению $\mu(x_{ij})$.

Разложив функцию (8) в ряд Макларена и ограничившись первыми членами ряда, получим

$$P_i^{\text{устр}} = P_i^{\text{устр}}(0) + \sum_{i=1}^{m} \frac{\partial P_i^{\text{устр}}}{\partial x_{ij}} \cdot x_{ij}. \tag{9}$$

где $P_i^{\text{устр}}(0)$=0 – вероятность устранения *i*-й угрозы при невыполнении требований и СЗИ;

$\frac{\partial P_i^{\text{устр}}}{\partial x_{ij}}$=$\alpha_{ij}$ – величина, характеризующая степень влияния *j*-го требования на вероятность устранения *i*-й угрозы (важность выполнения *j*-го требования для устранения *i*-й угрозы), $0 \le \alpha_{ij} \le 1$; $\sum_{i=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1,n}$.

После подстановки в (9) соответствующих значений получаем

$$P_i^{\text{устр}} = \sum_{j=1}^{n} \alpha_{ij} \cdot \bar{x}_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}). \tag{10}$$

Окончательно формула (5) для оценки величины $\overline{W}$ предотвращенного ущерба принимает вид

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \bar{\lambda} q_i \alpha_{ij} \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \bar{\lambda} q_i \alpha_{ij} \mu(x_{ij}). \tag{11}$$

Таким образом, задача синтеза СЗИ в виде (1), (2) сводится к оптимальному обоснованию количественных и качественных требований к СЗИ при допустимых затрат и принимает следующий вид [4]:

Найти

$$\max \overline{W}(x_0, \ i = \overline{1,n}, \ j = \overline{1,m}) \tag{12}$$

при ограничении

$$C(x_{ij}) \le C_{\text{доп}}; \ i = \overline{1,n}; \ j = \overline{1,m}.$$

При отсутствии информации об угрозах для решения задачи (12) может быть использован показатель вида

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \alpha_{ij} \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \alpha_{ij} \mu(x_{ij}).$$

4. Этапы решения задачи.

В соответствии с формулировкой задачи (12) основными этапами ее решения являются:

– сбор и обработка экспертной информации о характеристиках угроз: частоте появления *i*-й угрозы $\bar{\lambda}$ и ущербе q_i, $i = \overline{1,n}$;

– сбор и обработка экспертной информации [7] для определения важности выполнения *j*-го требования для устранения *i*-й угрозы α_{ij} и функции принадлежности x_{ij}, $i = \overline{1,n}$; $j = \overline{1,m}$;

– оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований x_{ij}, $i = \overline{1,n}$; $j = \overline{1,m}$;

– разработка математической модели и алгоритма выбора рационального варианта построения СЗИ в соответствии с постановкой (12) как задачи нечеткого математического программирования.

СПИСОК ЛИТЕРАТУРЫ

1. Левкин И.М., Левкина С.В., Сорокина Е.А. Информационно-признаковое моделирование угроз национальной безопасности// Вестник Академии военных наук. Северо-Западное отделение, 2013.
2. Бабенко Л.К., Басан А.С., Журкин И.Г., Макаревич О.Б. Защита данных геоинформационных систем: учеб. пособие для студентов вузов / Под ред. И.Г. Журкина. - М.: Гелиос АРВ, 2010. - 336 с., ил.
3. Левкин И.М., Микадзе С.Ю. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе// VIII Санкт-Петербургская межрегиональную конференцию «Информационная безопасность регионов

России (ИБРР-2013)», 2013.
4. Татарникова Задача синтеза комплексной системы защиты информации в ГИС//Ученые записки РГГМУ, №30, 2013. С. 204-211.
5. Бескид П.П., Татарникова Т.М. О некоторых подходах к решению проблемы авторского права в сети Интернет//Ученые записки РГГМУ, №15, 2010. С.
6. Татарникова Т.М., Яготинцева Н.В. Постановка задачи синтеза комплексной защиты от воздействия угроз в телекоммуникационной системе //Информационные технологии и системы: управление, экономика, транспорт, право. Межвузовский сборник научных трудов. Выпуск 1(9), СПб, 2011.
7. Татарникова Т.М., Яготинцева Н.В. Принципы организации экспертной системы выбора надежных средств защиты информации VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». Санкт-Петербург, 26-28 октября 2011 г.

ЦЕЛОЧИСЛЕННАЯ ОЦЕНКА КОЛИЧЕСТВА ИНФОРМАЦИИ В ЗАДАЧАХ СТЕГАНОГРАФИИ И РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ

Харинов Михаил Вячеславович, Заболотский Вадим Петрович,
Санкт-Петербургский институт информатики и автоматизации РАН,
СПИИРАН, Россия, Санкт-Петербург, 14-я линия ВО, д. 39,
e-mail: khar@iias.spb.su, lai@iias.spb.su.

Аннотация: В статье анализируются этапы создания модели цифрового сигнала как запоминающей среды для хранения информации и обобщаются ее основные понятия: формальное определение количества информации в элементе сигнала; b) модель сигнала с цифровой памятью; c) аналитические соотношения для приращения суммарной квадратичной ошибки; d) аппарат вычислений в терминах динамических деревьев Слэйтора-Тарьяна.

Ключевые слова: *количество информации; шенноновская оценка; оценка по Р.Хартли; пиксель; кластеризация пикселей; сегментация изображения; метод Уорда; метод Оцу; модель Мамфорда-Шаха; иерархия; суммарная квадратичная ошибка; инвариантность; изоморфизм; изотонное преобразование*

INTEGER ESTIMATION OF INFORMATION QUANTITY IN STEGANOGRAPHY AND IMAGE RECOGNITION TASKS

Kharinov Mikhail V., Zabolotsky Vadim P.
The Saint-Petersburg Insitutete for Informatics and Automation RAS,
SPIIRAS, Russia, Saint-Petersburg, 14 Linia 39.
e-mail: khar@iias.spb.su, lai@iias.spb.su.

Abstract: The article outlines the development stages of the model describing a digital signal as a peculiar medium for information storage, and summarizes the basic concepts: a) a formal definition of integer information quantities in elements of a signal; b) a model of digital signal memory; c) analytical expressions for the increments of the total squared error; d) a computing toolkit of Sleator-Tarjan dynamic trees.

Key words*: information quantity; Shannon estimation; estimation by R. Hartley; pixel; pixel clustering; image segmentation; Ward's method; Otsu method; Mumford-Shah model; hierarchy; total squared error; invariance; isomorphism; isotone transform.*

В работе развивается подход [1] к оценке количества информации в элементе сигнала и объединяются результаты исследований по проблеме количественной интерпретации понятия информации изображений, полученные в течение 25 последних лет. В последнем десятилетии 20-го века решены технические проблемы вычислений, в первом десятилетии 21-го века изучена проблема встраивания в сигнал произвольных сообщений по заданному алгоритму и, в настоящее время, решается проблема адекватного представления, количественной оценки и обработки естественной информации, содержащейся в сигналах различной природы.

В 90–х годах в СПИИРАН впервые в практике обработки сигналов начали применять динамические деревья Слэйтора-Тарьяна, которые не имеют альтернатив при вычислениях с иерархией разбиений сигнала. Благодаря структурам данных на основе указанных деревьев оказалось возможным создать обучаемые программы многоуровневой адаптивной сегментации изображений в условиях, по современным меркам, катастрофического недостатка памяти и быстродействия тогдашних ЭВМ. При этом именно недостаток памяти вызывал ее дополнительные затраты на хранение упакованных копий данных и снижал скорость обработки из-за необходимости организации буферного обмена данными с внешними носителями. С развитием компьютеров отмеченные трудности исчезли, а применение динамических деревьев стало более эффективным не только за счет исключения чрезмерного расхода памяти, но и за счет того, что для обработки иерархии разбиений изображений стало с избытком хватать оперативной памяти персонального компьютера. Постепенно динамические деревья внедряются в обработку информации, в основном за рубежом, где, в зависимости от приложений, именуются «Sleator-Tarjan dynamic trees», «Disjoint sets», «Persistent data structures» или «Splay tree».

Используя аппарат динамических деревьев для выполнения необходимых экспериментов, авторы, на примере цифровых изображений, продолжили исследование в задаче стеганографического встраивания информации в сигнал, которая противоположна задаче извлечения информации из сигнала при распознавании. При этом приобрели необходимый опыт обработки, так называемой, «глобально-локальной информации», т. е. организации вычислений с взаимосогласованным учетом свойств множества элементов сигнала в целом и каждого элемента сигнала в отдельности [2]. В результате удалось построить модель сигнала с порождаемой сигналом цифровой памятью, которая в 2006–2008 г. была опубликована в монографии [3] и защищена двумя патентами РФ (№2006119273 и №2006119146). Модель удобна тем, что встраивание и извлечение сообщений в «виртуальную» память сигнала выполняется по аналогии с записью и чтением информации из обычной цифровой памяти, причем максимальное число бит, которые можно встроить в данный элемент сигнала, оценивается целым числом, которое трактуется как оценка количества информации. Как мы установили экспериментально в [4], предложенная целочисленная оценка количества информации, как правило, принимает промежуточные значения между классическими оценками по Р. Хартли и К. Шеннону, что является обнадеживающим результатом.

В текущем десятилетии авторы вернулись к задачам извлечения информации из сигнала, в том числе к модели сигнала с цифровой памятью в приложении к, так называемой, «проблеме сегментации» цифрового изображения. Поводом для возобновления исследований послужило явное улучшение сегментации при коррекции имеющегося ПО иерархической сегментации с учетом модели Мамфорда-Шаха [5–9] в версии А.С. Бугаева [10]. При этом эффект обеспечивался благодаря вычислению иерархии приближений изображения посредством минимизации суммарной квадратичной ошибки *E*. Затем, реализовав вычисление оптимальных приближений изображения в вариантах метода Оцу [11,12], удалось показать [13,14], что минимизацию E в модели Мамфорда-Шаха можно существенно улучшить и при этом аппроксимировать оптимальные приближения квазиоптимальными иерархическими приближениями, которые сохраняют свойство выпуклости последовательности значений суммарной квадратичной ошибки E. Важным дополнительным аргументом в пользу применения иерархии квазиоптимальных приближений является то, что они, в отличие от неиерархических оптимальных приближений, представимы в изоморфном инвариантном виде [15], что необходимо для использования модели сигнала с цифровой памятью. Характерно, что принципиальные отличия алгоритмов генерации квазиоптимальных приближений от известных алгоритмов [16], с точки зрения программирования незначительны. Однако именно эти отличия обеспечивают получение приближений с установленными формальными свойствами выпуклости и др. [15,17], что способствует унификации программ для обработки изображений и других сигналов.

По всей видимости, на современном уровне теории и практики обработки сигналов для получения эффективных методов извлечения информации особенно актуальны критический анализ, обобщение, объединение и обоснованный выбор алгоритмов из многообразия используемых. При этом обсуждаемая разработка опирается на:

- формальное определение количества информации в элементе сигнала [1,4,15];
- модель сигнала с цифровой памятью [3];
- аналитические соотношения для приращения суммарной квадратичной ошибки [18,19];
- аппарат вычислений в терминах динамических деревьев Слэйтора-Тарьяна [3,20].

Целочисленная оценка количества информации решает фундаментальную научную проблему толкования бита как минимальной единицы измерения количества информации. Проблема характерна для классической интерпретации количества информации в элементе сигнала [1] по Р. Хартли, К. Шеннону и комбинаторном подходе, в которых количество информации выражается вещественным числом. Для целочисленной оценки количества информации мы применяем детерминированный подход, но, в отличие от комбинаторного подхода, оцениваем не суммарное количество информации в сигнале, а число бит информации, которое сопоставляется элементам сигнала (пикселям изображения, самплам аудиосигнала и пр.). Идея сопоставления последовательности бит информации элементам сигнала сводится к последовательному считыванию альтернативных двузначных значений с каждого элемента сигнала. При этом полагается, что любой нетривиальный сигнал по определенному алгоритму разделяется на два вложенных сигнала, различающихся средними значениями своих элементов. Под *тривиальным* сигналом понимается сигнал, состоящий из одинаковых элементов, который под действием алгоритма дихотомического разделения сигнала не меняется и является терминальным сигналом в получаемой для каждого исходного сигнала иерархии вложенных сигналов. Считается, что при каждом разделении нетривиального сигнала надвое, с элементов вложенного сигнала с меньшей величиной среднего значения считывается нулевое значение бита информации, а с элементов вложенного сигнала с большей величиной среднего значения считывается альтернативное значение бита информации. Количество значений, считанных с данного элемента сигнала, принимается в качестве оценки количества информации, содержащейся в этом элементе сигнала. При этом целочисленное количество информации в элементе сигнала определяется как число неповторяющихся нетривиальных вложенных сигналов из заданной дихотомической иерархии, в которых встречается рассматриваемый элемент [15]. В частности, элементы тривиального сигнала содержат нулевое

количество информации. Как показано в [15], для пикселей цифрового изображения целочисленная оценка количества информации, согласно приведенному определению, согласуется с оценками по формулам Р. Хартли и К. Шеннона и оказывается ближе к той или другой, в зависимости от способа вычисления иерархии вложенных сигналов по исходному сигналу. Поэтому предложенную целочисленную оценку количества информации можно считать вариантом интерпретации классических вещественных оценок по формулам Р. Хартли и К. Шеннона, полученной на основе аппроксимации сигнала иерархической последовательностью кусочно-постоянных приближений. Развитие предложенной интерпретации заключается в том, что для каждого приближения сигнала информация разделяется на две компоненты при неизменном суммарном количестве информации. Одну компоненту составляют коды информации, содержащиеся во вложенных сигналах, на которые разделяется исходный сигнал, а вторая компонента является информацией кусочно-постоянного приближения сигнала, образованного вложенными сигналами с усредненными значениями своих элементов. При этом общее количество информации в сигнале, очевидно, превышает или, по крайней мере, совпадает с суммарным количеством информации во вложенных сигналах, что можно трактовать как усиленное свойство монотонности количества информации. Таким образом, в нашей интерпретации количество информации сигнала, помимо аддитивности, характеризуется усиленными аксиоматическими свойствами неотрицательности и монотонности.

Согласно модели [3], коды извлекаемой из сигнала информации содержатся в свойственной сигналу цифровой «виртуальной» памяти, в которой составляют *инвариантное изоморфное* представление сигнала, т.е. новый сигнал, который не зависит от определенных искажений исходного сигнала и сохраняет его основные свойства. В отличие от первоначальной версии модели для стеганографического встраивания искусственных сообщений [3,4], в современной версии модели сигнала с цифровой памятью для достоверного извлечения информации из исходного сигнала по-новому строится иерархия вложенных сигналов [15,17]. Решение достигается благодаря постановке и решению задачи многокритериальной условной оптимизации, состоящей в аппроксимации последовательности оптимальных приближений иерархической последовательностью квазиоптимальных приближений при дополнительных ограничениях на число сегментов и других параметров.

Алгоритмы представления сигнала посредством его иерархического разбиения на вложенные сигналы с минимальным значением суммарной квадратичной ошибки обосновываются элементарными формулами, которые описывают приращение ΔE_{merge} суммарной квадратичной ошибки E при слиянии двух вложенных сигналов в один, ΔE_{split} – приращение E при выделении нескольких элементов сигнала в дополнительный сигнал, вложенный в исходный, и $\Delta E_{correct}$ – приращение E при исключении нескольких элементов из одного вложенного сигнала и включении их в число элементов другого сигнала [19]. На сегодняшний день наиболее употребительной является формула [10] для ΔE_{merge} при слиянии сигналов 1 и 2 из n_1 и n_2 элементов, которые имеют средние значения I_1 и I_2, соответственно:

$$\Delta E_{merge} = \frac{\|I_1 - I_2\|^2}{\frac{1}{n_1} + \frac{1}{n_2}} \geq 0 \ ,$$

где символ $\| \ \|$ обозначает евклидово расстояние. Именно величина ΔE_{merge} минимизируется при оптимизации кусочно-постоянных приближений изображения посредством связных сегментов в версии [10] модели Мамфорда-Шаха [5–9]. В версии [7] формула отличается аддитивным членом, а в FLSA версии [8,9] – множителем, которые вводятся для учета общей длины границ между сегментами изображения. В нашей интерпретации снимаются ограничения на минимизацию E, характерные для перечисленных решений, и эффект применения обсуждаемой формулы усиливается, особенно, в сочетании с остальными двумя формулами [19]. Вместе с тем, как установлено в [17], в предельном случае одномерного сигнала, результат вычислений по алгоритму [16] анализа последовательных столбцов гистограммы оказывается тем же самым, что и в общем случае тотального перебора пар сигналов, если эвристический критерий [16] заменить условием

$$\Delta E_{merge} = \min.$$

Таким образом, аналитическое обоснование позволяет уточнить алгоритмы обработки и подсказывает их эффективную программную реализацию.

В связи с уточнением постановки задачи аппроксимации сигнала иерархией квазиоптимальных приближений, состоящих из вложенных сигналов, которые обрабатываются независимо друг от друга как самостоятельные сигналы, оказалось необходимым существенно переработать структуру данных и

алгоритмический аппарат вычислений в терминах динамических деревьев Слэйтора-Тарьяна [3,20], что планируется описать в отдельных публикациях.

Работа в целом представляет результаты междисциплинарных исследований в области встраивания и извлечения информации, направленные на построение математической модели сигнала как запоминающей среды для цифровых изображений, аудиосигналов, а также других сигналов различной природы.

СПИСОК ЛИТЕРАТУРЫ

1. Юсупов Р.М. Теоретические основы прикладной кибернетики. Выпуск 1. Элементы теории информации. – Л.: типография ВИКА им. А.Ф.Можайского, – 1973. – 110 с.
2. Абламейко, С.В., Недзьведь А.М., Белоцерковский А.М., Руцкая Е.А. Сегментация трехмерных изображений компьютерной томографии на основе глобально-локальной информации // Вестник Белорусского государственного университета. Сер. 1, Физика. Математика. Информатика. – 2009. – №1. – С.58–64.
3. Харинов М.В. Запоминание и адаптивная обработка информации цифровых изображений / Под ред. Р.М. Юсупова. – СПб.: Изд-во С.Петерб. ун-та, – 2006. – 138 с.
4. Харинов М.В., Заболотский В.П. Стеганографическая защита документов на основе модели запоминания информации изображения // Информация и связь. – 2008. – №1. – С.77–81.
5. Mumford D., Shah J. Boundary detection by minimizing functionals, I // Proc. IEEE Comput. Vision Patt. Recogn. Conf. – 1985. – San Francisco, – P. 22–26.
6. Mumford D., Shah J. Optimal Approximations by Piecewise Smooth Functions and Associated Variational Problems // Communications on Pure and Applied Mathematics. – 1989. – Vol. XLII, – №4, – P. 577–685.
7. Koepfler G., Lopez C., Morel J. A Multiscale Algorithm for Image Segmentation by Variational Method // SIAM Journal on Numerical Analysis. – 1994. – Vol. 31, – №1, – P. 282–299.
8. Crisp D.J., Tao T.C. Fast Region Merging Algorithms for Image Segmentation // The 5th Asian Conf. on Computer Vision (ACCV2002). Melbourne, Australia, 23–25 January 2002. – P. 1–6.
9. Robinson B.J., Redding N.J., Crisp D.J. Implementation of a fast algorithm for segmenting SAR imagery // Scientific and Technical Report, Australia: Defense Science and Technology Organization, Australia, 01 January 2002. – 42 p.
10. Бугаев А.С., Хельвас А.В. Поисковые исследования и разработка методов и средств анализа и автоматического распознавания потоковой информации в глобальных информационных системах. Шифр «Лацкан» // Отчет по НИР. М.: МФТИ, – 2001. – Том 1, – 140 с.
11. Otsu N. A Threshold Selection Method from Gray–Level Histograms // IEEE Transactions on systems, MAN, and CYBERNETICS. – 1979. – Vol. SMC–9, – №1, – P. 62–66.
12. Ping-Sung Liao, Tse-Sheng Chen, Pau-Choo Chung A Fast Algorithm for Multilevel Thresholding // J. Inf. Sci. Eng. – 2001. – Vol. 17, – №5, – P. 713–727.
13. Kharinov M.V. Image Segmentation Method by Merging and Correction of Sets of Pixels // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications. Pleiades Publishing, Ltd. – 2013. – Vol. 23. – №3, – P. 393-401.
14. Kharinov M.V. Image segmentation by optimal and hierarchical piecewise constant approximations // 11th International Conference on Pattern Recognition and Image Analysis: New Information Technologies (PRIA–11–2013) / Proc. of the 11-th. Int. Conf., – Samara: IPSI RAS, September 23-28 2013. – Vol. 1. – P. 213–216.
15. Харинов М.В. Количество информации в пикселе цифрового изображения // Вестник Бурятского государственного университета. Математика, информатика. – 2013. – №2. – С. 105-114. ISSN 2304-5728
16. Arifin A.Z. and Asano A. Image segmentation by histogram thresholding using hierarchical cluster analysis // Pattern Recogn. Letters. – 2006. – №27(13), – P. 1515–1521.
17. Kharinov M.V. Hierarchical pixel clustering for image segmentation // arXiv preprint, arXiv: 1401.5891, 24 Jan 2014. – 5 p. URL: http://arxiv.org/ftp/arxiv/ papers/1401/1401. 5891.pdf
18. Харинов М.В. Обобщение трех подходов к оптимальной сегментации цифрового изображения // Труды СПИИРАН. – 2013. – Вып. 2(25). – С. 294–316.
19. Харинов М.В. Модель локализации объектов на цифровом изображении // Вестник Бурятского государственного университета. Математика, информатика. – 2013. – №9. – С. 182–189. ISSN 1994-0866
20. Galiano P., Kharinov M., Vanurin S. Application of Sleator-Tarjan dynamic trees in Monitoring system for Arctic region based on remote sensing data // Information Fusion and Geographic Information Systems (IF&GIS'2013) / Proceedings of the 6th International Workshop on Information Fusion and Geographic Information Systems: Environmental and Urban Challenges. 12–15 May 2013, St. Petersburg (Russia): Springer, LNG&C, – 2014. – P. 137–147.

УДК 519.7

ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ РАЗВИТИЯ ИКТ И ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Шишкин Владимир Михайлович[1], Абросимов Иван Константинович[2],
[1.]Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, д. 39,
[2.]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mails: vms@iias.spb.su, ivnabr@yandex.ru.

Аннотация: В статье рассмотрены предпосылки и показана возможность использования аппарата обыкновенных дифференциальных уравнений в качестве инструмента объективного анализа и прогноза для моделирования процессов динамического взаимодействия в системе факторов, связанных с развитием ИКТ и обеспечением национальной безопасности. Представлены некоторые результаты моделирования, показавшие правдоподобность поведения модели и её пригодность для анализа развития ситуаций при альтернативных сценариях.

Ключевые слова: *макромоделирование; дифференциальные уравнения; правдоподобность поведения.*

DYNAMIC MODEL OF INTERACTION SYSTEM OF IT DEVELOPMENT AND NATIONAL SECURITY ENSURING

Shishkin Vladimir Michailovich[1], Abrosimov Ivan Konstantinovich[2],
[1] St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14 line, 39,
[2] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
e-mails: vms@iias.spb.su, ivnabr@yandex.ru.

Abstract: Prerequisites are considered and suitability is shown for ordinary differential equations as the tool to objective analysis and the forecast for modeling of dynamic interaction processes in a system of the factors, those connected with IT development and national security ensuring. Some results of modeling are presented which have confirmed plausibility of model behavior and its suitability for the situations dynamics analysis under alternative scenarios.

Key words: *macromodelling; differential equations; plausible behavior.*

Мотивы исследования

Исключительная роль, которую приобрели в современном мире информационно-коммуникационные технологии (ИКТ) практически во всех областях деятельности человечества, стала очевидным фактом. Они инкорпорированы во все системы жизнеобеспечения и управления государства, регионов, производственные процессы, в большинство видов технических устройств и технологического оборудования, вошли в повседневный быт значительной части населения.

Очевидно также, что развитие и распространение ИКТ сопровождается нарастанием и усложнением плохо решаемых, как показывает практика, проблем информационной безопасности разного масштаба, от индивидуального до глобального. Информационная безопасность (ИБ) стала не просто структурной составляющей национальной безопасности, но неотъемлемо присутствует во всех её аспектах. Последние годы демонстрируют отчетливую тенденцию того, что обеспечение ИБ на различных её уровнях и в разных аспектах приобретает черты противоборства и становится непрерывным процессом. Более того, собственно защита становится недостаточной для поддержания ИБ, технология её обеспечения требует уже тех или иных атакующих воздействий на потенциального противника, «исходя из старого лозунга: нападение лучший способ обороны» [1].

При этом существуют практически взаимоисключающие взгляды на стратегию развития ИКТ в России, а, следовательно, и на проблематику ИБ, хотя в последнее время мнения, оппозиционные декларируемой государственной политике, стали менее заметны. С одной стороны, прилагаются усилия по воссозданию импортозамещающего производства отечественной компонентной базы СВТ, коммуникационного оборудования, разработке ОС, без чего трудно говорить о поддержании приемлемого уровня ИБ, во всяком случае, в сфере государственного управления, обороны, функционирования критически важных систем и объектов. С другой стороны, утверждается неэффективность подобных мер при перенасыщенном глобальном рынке средств ИКТ.

Достаточно, как пример, вспомнить подготовленную вскоре после утверждения «Доктрины информационной безопасности», видимо, как её контр-альтернатива, одиозную «Белую книгу информационных технологий» (2000 г.), в которой единственной областью ИКТ, достойной для развития в России был признан аутсорсинг ПО. Или относительно недавние (2009 г.) намерения исключить из приоритетных направлений развития науки, технологий и техники в Российской Федерации направление «Информационно-телекоммуникационные системы», парадоксально мотивированные тем, что «Россия … отстает от развитых стран по уровню научных исследований в области информационно-коммуникационных технологий». Причём все эти инициативы исходили от около правительственных структур.

В силу этого, необходимы инструменты объективного анализа и прогноза, а именно, средства математического моделирования. Связав в систему динамического взаимодействия некоторый набор существенных в определённом контексте факторов, расчётным путём можно будет обеспечить возможность оценки развития ситуации при альтернативных сценариях, воспроизводить различные варианты поведения сторон, оценивать эффективность управляющих воздействий и т.д.

Математический аппарат и основные предположения о модели

В первом приближении, поскольку многие системы, изменение состояния которых согласовано с законами сохранения, могут быть описаны на языке обыкновенных дифференциальных уравнений [2], это может быть простейшая система таких уравнений. Опыт применения подобного рода динамических моделей в различных предметных областях, в том числе плохо формализуемых, имеет уже достаточно давнюю историю, показав их, по крайней мере, познавательную и прогностическую полезность. Поэтому естественно попытаться применить этот аппарат для моделирования и анализа

динамики взаимодействия развития ИКТ и обеспечения национальной безопасности (НБ), а в дальнейшем – информационной борьбы, причем, как в макро масштабе, например, государственной политики, так и на технологическом уровне.

Прежде всего, при использовании данного аппарата необходимо определить фазовое пространство, что является непростой и неоднозначно решаемой задачей. Тем не менее, некоторые из фазовых переменных, скорее всего, должны быть в их составе. Из вышесказанного следует, что при макро-моделировании трудно обойтись без учёта уровня информатизации, развития ИКТ, уровня НБ, неразрывно связанного с уровнем ИБ, а значит с уровнем развития ИКТ. А в силу того, что пассивная оборона не способна обеспечить НБ, система её обеспечения должна обеспечивать возможность создания угроз НБ противника. Поэтому следует включить в число фазовых переменных уровень системы обеспечения НБ и ресурс, идущий на поддержание системы обеспечения НБ. Источником пополнения ресурсов естественно предложить уровень социально-экономического развития (СЭР), поэтому он должен войти в модель в качестве одной из фазовых переменных.

Построение модели и результаты моделирования

В первоначальной версии нашей модели [3], ещё не включавшей процессы противоборства, в качестве содержательной основы была использована структурная схема, основанная на схеме из [4], иллюстрирующая взаимодействие развития ИКТ и обеспечения НБ через систему других разнонаправленно действующих факторов. Даже в образном виде она позволяла видеть, что при отсутствии сбалансированности составляющих процесса, недооценке угроз, учитывая опосредованные обратные связи, национальной безопасности и в целом социально-экономическому развитию может быть нанесен ущерб. В упрощённом для удобства моделирования виде эта схема приобрела следующий вид (рисунок 1).

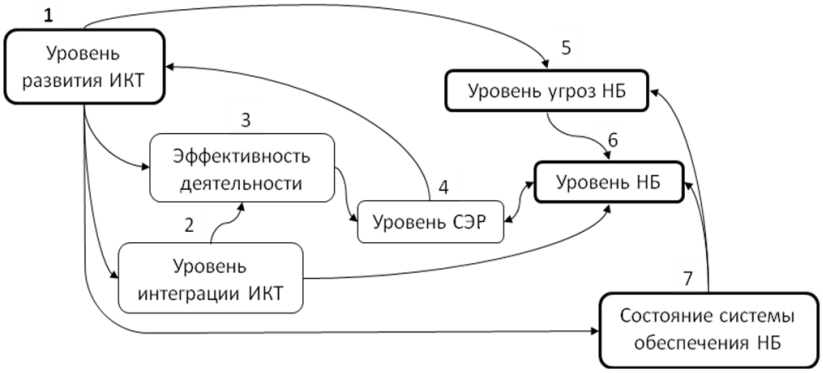


Рис. 1. Структурная схема модели системы взаимодействия развития икт и обеспечения НБ

В качестве фазовых переменных выступают элементы структурной схемы:

y_1 – уровень развития ИКТ;

y_2 – уровень интеграция ИКТ;

y_3 – эффективность деятельности по повышению уровня СЭР;

y_4 – уровень СЭР;

y_5 – уровень угроз НБ;

y_6 – уровень НБ;

y_7 – состояние системы обеспечения НБ.

Для начала модель была представлена системой семи обыкновенных дифференциальных уравнений первого порядка следующего вида:

$$\dot{y} = P^T y + Q^T \dot{y}, \tag{1}$$

где $\mathbf{y}$ – вектор фазовых переменных, в качестве которых выступают элементы указанной структурной схемы; $\mathbf{P} = \{p_{ij}\}$ – матрица, в которой p_{ij} – коэффициенты влияния y_i на динамику y_j, для $i \neq j$, а на главной диагонали расположены собственные потенциалы i-го фактора p_i (потенциал представляет собой приращение или убыль относительно начального состояния в единицу времени);

$Q = \{q_{ij}\}$ – матрица, в которой q_{ij} – коэффициенты влияния динамики y_i на динамику y_j, $i \neq j$, $q_{ii} = 0$.

Для упрощения поиска области устойчивости значения коэффициентов фиксировались соответственно разным сценариям развития ситуации, а для проверки устойчивости использовался критерий Гурвица.

Тестовые расчёты показали правдоподобное поведение модели в автономном режиме, что позволяет исследовать её при различных сценариях управлений и более содержательном назначении коэффициентов.

Общее решение системы (1) имеет вид:

$$y_i = \sum_{m=1}^{r} \sum_{l=0}^{k(s_m)-1} C_{ml}^{i} t^l e^{s_m t},\ C_{ml}^{i} = const\ ,$$

где: r – число различных корней характеристического полинома; $k(s_m)$ – кратность корня.

Несмотря на то, что решение этой системы имеет определённую форму, возникают трудности, связанные с поиском корней полинома (по теореме Абеля-Руффини корни полинома степени выше четвертой нельзя найти в радикалах), порядок которого равен порядку системы, что вынуждает нас прибегать к численным методам решения данной системы. Численное решение можно провести, например, с помощью систем компьютерной алгебры.

Исходя из содержательного смысла модели, можно сделать некоторые предположения и наложить ограничения на её элементы:

1. Несколько упрощая, будем считать, что значения фазовых переменных влияют только на собственную динамику, т.е. P – диагональная матрица.
2. Факторы 2, 3, 4, 6 – пассивны, и соответствующие им $p_i = 0$.
3. Уровень угроз НБ только возрастает, поэтому $p_5 > 0$.
4. Однозначная направленность взаимовлияния факторов позволяет для всех q_{ij} кроме q_{26}, зафиксировать знаки соответствующих членов в уравнениях, тогда $q_{ij} > 0,\ i \neq 2,\ j \neq 6$.
5. На коэффициенты p_1, p_7, q_{26} ограничения по знаку не налагаются.
6. Фазовые переменные имеют смысл отношения текущего значения к начальному, поэтому $y_i \geq 0$, а начальные условия $y_i(0) = 1$.

Тогда система уравнений запишется в следующем виде:

$$\begin{cases} \dot{y}_1 = p_1 y_1 + q_{41}\dot{y}_4, \\ \dot{y}_2 = q_{12}\dot{y}_1, \\ \dot{y}_3 = q_{13}\dot{y}_1 + q_{23}\dot{y}_2, \\ \dot{y}_4 = q_{34}\dot{y}_3 + q_{64}\dot{y}_6, \\ \dot{y}_5 = p_5 y_5 + q_{15}\dot{y}_1 - q_{75}\dot{y}_7, \\ \dot{y}_6 = q_{26}\dot{y}_2 + q_{46}\dot{y}_4 - q_{56}\dot{y}_5 - q_{76}\dot{y}_7, \\ \dot{y}_7 = p_7 y_7 + q_{17}\dot{y}_7. \end{cases} \tag{2}$$

На рисунке 2 показаны некоторые результаты моделирования на системе (2) в виде трёх диаграмм, где t - время, p_1 – потенциал развития ИКТ, и y_6 – уровень НБ (см. выше).

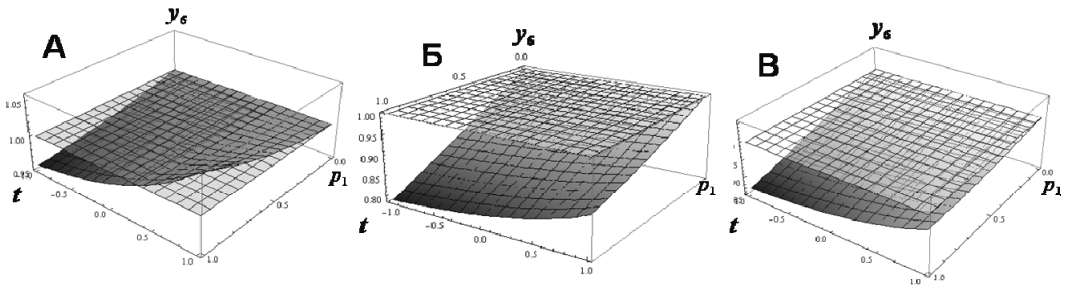


Рис. 2. Результаты моделирования.

На диаграмме А представлен благоприятный вариант развития ситуации (положительный потенциал системы обеспечения НБ, $p_7 > 0$). Как видим, тогда уровень НБ ($y_6 > 0$) монотонно растёт при достаточных потенциалах развития ИКТ (p_1) и системы обеспечения НБ.

Диаграмма Б - неблагоприятное развития ситуации (отрицательный потенциал системы обеспечения НБ, $p_7 < 0$) – показывает очевидное: любой вариант развития ИКТ при деградации системы обеспечения НБ приводит к резкому снижению уровня безопасности.

Наконец, на диаграмме В - промежуточный вариант развития процесса (нулевой потенциал системы обеспечения НБ), видно, что стагнация системы обеспечения НБ, как и её деградация (Б), в любом случае ведёт не к фиксации, а к снижению уровня национальной безопасности.

Таким образом, как оказалось, построенная модель, несмотря на предельную простоту, дала правдоподобные результаты, показав возможность применения дифференциальных моделей для решения задач, подобных рассмотренной. Разумеется, интерпретация результатов почти очевидна и без расчётов на модели, но объективный инструмент всегда убедительнее вербальных доводов и подкрепляет их.

Заключение

Таким образом, построенная модель, несмотря на предельную простоту, дала правдоподобные результаты, показав возможность применения дифференциальных уравнений для решения задач, подобных рассмотренной. Интерпретация результатов моделирования почти очевидна и без расчётов на модели, но объективный инструмент всегда убедительнее вербальных доводов и подкрепляет их.

Для целей моделирования информационной борьбы нами исследуются и другие типы моделей динамических систем, в частности, с использованием физических аналогий, моделей популяционной динамики и других. Продолжается поиск наиболее подходящих для разных ситуаций вариантов фазового пространства борьбы в инфосфере и критериев управления.

СПИСОК ЛИТЕРАТУРЫ

1. Юсупов Р.М, Шишкин В.М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. Вып. 6. – СПб.: Наука, 2008. – С.11–23.
2. Моисеев Н.Н. Универсум. Информация. Общество. – М.: Устойчивый мир, 2011. – 200с.
3. Шишкин В.М., Абросимов И.К. Динамическая модель системы взаимодействия развития ИКТ и обеспечения национальной безопасности // Информационная безопасность регионов России (ИБРР–2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2013.: Материалы конференции / СПОИСУ. – СПб., 2013. – С. 25.
4. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь, №1, 2010. – С. 27–35.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3

ОБЩИЕ ВОПРОСЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СХЕМ ПО СОСТАВНОМУ МОДУЛЮ

Березин Андрей Николаевич,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профеесора Попова, д. 5,
e-mail: a.n.berezin.ru@gmail.com.

Аннотация: В работе рассмотрены основные подходы к построению криптосхем на основе двух трудных задач. Описаны особенности нового подхода с использованием задачи дискретного логарифмирования по составному модулю. Показана применимость нового подхода для построения схем цифровой подписи, слепой цифровой подписи, протоколов с нулевым разглашением, открытого распределения ключей, открытого и коммутативного шифрования с использованием нового подхода. Предлагаемый подход применим для построения криптосхем с открытым ключом всех типов, обеспечивает увеличение производительности протоколов цифровой подписи и сокращение размеров подписи по сравнению с известными криптосхемами, основанными на трудности одновременного решения задач факторизации и дискретного логарифмирования.

Ключевые слова*: задача факторизации; задача дискретного логарифмирования; задача дискретного логарифмирования по составному модулю; цифровая подпись; шифрование с открытым ключом; две трудные задачи.*

GENERAL ITEMS ON DESIGNING THE COMPOSITE-MODULO CRYPTOSCHEMES

Berezin Andrey,
The St-Petersburg State Electrotechnical University «LETI»,
Russia, St-Petersburg, Professor Popov str. 5,
e-mails: a.n.berezin.ru@gmail.com.

Annotation: There are considered main approaches to constructing cryptoschemes based on two hard problems and described peculiarities of using the problem of finding discrete logarithm modulo a composite number. It is shown the applicability of such approach for constructing the digital signature, public encryption, zero knowledge, and public key agreement protocols as well as for designing commutative encryption algorithms. The proposed approaches extends the type set of the cryptoschemes based on difficulty of simultaneous solving the factoring problem and the discrete logarithm modulo prime problem. It also provides reducing the signature size and increasing performance of the digital signature protocols.

Key words: *factorization problem; discrete logarithm problem; composite-modulo discrete logarithm problem; digital signature; public key encryption; two hard problems.*

Введение

Для обеспечения информационной безопасности широко используются криптографические схемы с открытым ключом [1]. Безопасность таких криптосхем основывается на следующих двух фактах: 1) решение используемой трудной задачи является вычислительно нереализуемой за приемлемое время (при использовании наилучшего алгоритма), то есть задача обладает достаточно высокой стойкостью W; 2) вероятность P появления вычислительно эффективного алгоритма для решения используемой трудной задачи в ближайшем будущем пренебрежимо мала. Это означает, что количественная характеристика безопасности криптосхем включает два параметра – стойкость и вероятность появления эффективного алгоритма решения используемой задачи. В качестве некоторого интегрального параметра безопасности вводится отношение W/P [2]. Повышение уровня безопасности криптосхемы может быть достигнуто за счёт увеличения сложности трудной задачи и уменьшения значения P. Вероятность P появления вычислительно эффективного алгоритма может быть значительно уменьшена, если взлом криптосхемы требует одновременного

решения двух независимых вычислительно трудных задач. Таким образом, для взлома криптосхемы потребуется появление сразу двух вычислительно эффективных алгоритмов решения.

Наиболее широкое распространение для построения различных типов криптосхем получили задачи факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ). Они также используются для построения криптосхем, взлом которых требует одновременного решения двух трудных задач.

В настоящем сообщении сравниваются различные подходы для построения криптосхем, на основе двух трудных задач, а также рассматриваются общие вопросы использования наиболее перспективного из них для построения криптографических схем по составному модулю.

1. Подходы к построению криптосхем на основе двух трудных задач

Наиболее очевидным подходом является комбинирование двух различных криптосхем (например, формирование двух электронных цифровых подписей (ЭЦП) к одному документу, шифрование сообщения последовательным выполнением двух различных алгоритмов). Очевидно, что данный подход имеет существенные недостатки, такие как дополнительные временные затраты на проведение вычислений, большого размера ЭЦП и необходимость хранения нескольких секретных ключей. Например, сообщение M подписывается сначала при помощи схемы ЭЦП RSA, а затем – ЭЦП Эль-Гамаля [1]. В случае использования ЭЦП RSA подписью к сообщению будет являться число, размер которого зависит от длины модуля (безопасный размер которого не менее 1024 бит). Из-за способа формирования подписи сократить размер не представляется возможным. При применении ЭЦП Эль-Гамаля подписью является пара чисел (в оригинальной схеме длина каждого параметра подписи зависит от длины модуля, по которому производят вычисления, при рекомендованной длине модуля 1024-2048 бит, длина подписи составит от 2048 до 4096 бит). Существуют модификации ЭЦП Эль-Гамаля [1], которые позволяют сократить размер подписи до 320-512 бит. В конечном итоге длина ЭЦП, сгенерированной при использовании такого подхода, составит в лучшем случае 1344 бита, а в худшем – 3072 бита. При этом возрастает вычислительная сложность расчёта ЭЦП.

Второй подход основан на внесении изменений в существующие криптосхемы, например, ЭЦП Эль-Гамаля, ЭЦП Шнорра, ГОСТ Р 34.10-94 [1]. В них используется ЗДЛ по простому модулю. Подход основан на возведении в некоторую степень параметра S и наложении дополнительных требований на модуль. Например, для ЭЦП Эль-Гамаля уравнение проверки подписи может выглядеть следующим образом $b^M = y^R R^\wedge (S^2) \bmod p$. Вместо простого модуля используется модуль со специальной структурой, функция Эйлера от которого содержит составное число n трудное для факторизации, из-за чего для вычисления корня потребуется решить ЗФ этого числа. Благодаря возведению в некоторую степень параметра S возникает необходимость одновременного решения ЗФ и вычисления квадратного корня по составному модулю $p-1$ (т.е. ЗФ и ЗДЛ одновременно). На основе данного подхода было предложено большое количество схем ЭЦП (например, описанные в работах [2,3,4]). Однако данный метод построения даёт низкую производительность по сравнению с базовыми криптосхемами и большой размер ЭЦП, который зависит от размера используемого модуля, и не всегда может быть сокращен. Этот подход характеризуется сложностью построения схем ЭЦП и не даёт общего принципа для построения криптосхем других типов.

2. Новый подход

Задача дискретного логарифмирования по составному модулю определяется некоторыми известными числами α, y, n и состоит в нахождении такого x, что выполняется следующее равенство $y = \alpha^x \bmod n$, где $n = pq$, p, q – сильные простые числа.

ЗДЛ по составному модулю принципиально отличается от ЗДЛ по простому модулю, т.к. для её решения могут быть использованы либо общие методы дискретного логарифмирования [5], имеющие экспоненциальную вычислительную сложность, либо метод сведения к ЗДЛ по простому модулю путём факторизации и решения ЗДЛ по простому модулю, имеющий субэкспоненициальную сложность. В случае появления прорывного метода решения ЗФ или ЗДЛ по простому модулю это не приведёт к взлому криптосхемы, основанной на ЗДЛ по составному модулю. При использовании составного модуля также необходимо учитывать возможность быстрой факторизации модуля с использованием расширенного алгоритма Евклида, поэтому значение α необходимо генерировать специальным образом [6], [7].

Ниже приведены 2 алгоритма выбора числа α:

1. Генерируем сильные простые числа p и q такие, что некоторое достаточно большое число γ делит $p-1$ и $q-1$. В качестве порядка α выбираем число, которое имеет порядок γ по модулю n. В этом случае значение γ может быть не секретным.

2. Генерируем сильные простые числа p и q такие, что существуют два достаточно больших числа γ', которое делит $p-1$, но не делит $q-1$, и γ'', которое делит $q-1$, но не делит $p-1$. В качестве b выбирается число, которое имеет порядок $\gamma = \gamma'\gamma''$ по модулю n. В этом случае значения $\gamma, \gamma', \gamma''$ должны быть секретными.

Данные ограничения на выбор α исключают возможность быстрой факторизации модуля n с использованием расширенного алгоритма Евклида [6], [7].

При использовании приведённых способов генерации α для решения ЗДЛ по составному модулю $\gamma = \alpha^x \bmod n$, необходимо решить ЗФ и две ЗДЛ по простому модулю (для p и q), заданных следующими двумя уравнениями:

$$y = \alpha^x \bmod q,$$
$$y = \alpha^x \bmod p.$$

Вычислительная сложность ЗФ определяется размером меньшего делителя модуля n, в то время как вычислительная сложность решения ЗДЛ зависит от выбора порядка α.

Очевидно, что в случае, когда порядок α одинаков для модулей p и q и равен γ, значение x является одинаковым для этих двух уравнений. Следовательно, если у злоумышленника есть алгоритм решения ЗФ, то ему для нахождения секретного x будет достаточно решить только одно из уравнений. То есть для нахождения секретного значения x достаточно будет решить ЗДЛ по модулю меньшего делителя числа n, это обеспечит вычислительную сложность примерно в 2 раза ниже, чем для ЗФ модуля n. Таким образом, размер множителей p и q должен быть примерно одинаковым, и в 2 раза больше чем в случае ЗФ, то есть соотношение размеров множителей p и q должно быть равно 2:2, например, по 2464 бита для обеспечения 128-битной стойкости. Это означает, что в рассматриваемом случае, вычислительная сложность ЗФ и ЗДЛ различается, однако каждая из задач будет не менее требуемого уровня стойкости криптосхемы, равного 2128 операций модульного умножения, что необходимо для того, чтобы взлом криптосхемы требовал одновременного решения ЗФ и ЗДЛ по простому модулю.

В случае $\gamma = \gamma'\gamma''$, для вычисления x необходимо решить два уравнения. Это обусловлено тем что решая одно из уравнений мы получим либо x_q либо x_p, причём $x_q \neq x_p \neq x$, так как порядок α по модулям p и q различен $\gamma' \neq \gamma''$. Значение x можно найти по китайской теореме об остатках из следующих двух уравнений

$$x \equiv x_p \bmod \gamma',$$
$$x \equiv x_q \bmod \gamma''.$$

Таким образом, основной вклад в вычислительную сложность ЗДЛ по простому модулю будет вносить больший множитель p. В этом случае возможно использование p и q с соотношением длин равным 1:2, то есть $|p| = 2|q|$. Тогда вычислительная сложность ЗДЛ по простому модулю p и сложность факторизации модуля n будут примерно равными. Для обеспечения вычислительной сложности 2128 операций модульного умножения для ЗДЛ и ЗФ необходимо выбирать два сильных простых числа q и p с длинной $|q| \approx 1232$ бит и $|p| \approx 2464$ бит. В обоих случаях для построения криптосхем со 128 битовой стойкостью значения $\gamma, \gamma', \gamma''$ должны иметь следующие размеры $|\gamma| \geq$ 256 бит, $|\gamma'| \geq 128$ бит, $|\gamma''| \geq 128$ бит.

Исходя из вышеизложенного, представляется интересным следующий подход к синтезу криптосхем, основанных на вычислительной сложности ЗФ и ЗДЛ, который состоит в применении известных и новых типов криптосхем с открытым ключом с использованием ЗДЛ по составному модулю. Более подробно о новом подходе и его применениях можно прочитать в работах [7], [8]. Далее остановимся на конкретных примерах криптосхем, построенных с использованием данного подхода.

3. Реализация схемы цифровой подписи

Пусть некоторый пользователь зарегистрировал свой открытый ключ (n, α, y) в удостоверяющем центре. Значение y вычисляется как $y = \alpha^x \bmod n$, где x является 256-битным

секретным ключом; $n = pq$, и α имеет 256-битный простой порядок γ по модулю n (γ не является секретным). Пользователь может подписать сообщение M, используя следующий протокол ЭЦП, аналогичный алгоритму ЭЦП Шнорра [9].

1. Сгенерировать случайное 256-битное k и вычислить $R = \alpha^k \bmod n$.

2. Используя 256-битную хэш-функцию F_H вычислить первый элемент подписи: $E = F_H(R\|M)$.

3. Вычислить второй элемент подписи $(E,S): S = k + xE \bmod \gamma$.

Процедура проверки подписи включает следующие шаги:

1. Вычислить $R^* = y^{-E}\alpha^S \bmod n$ и $E^* = F_H(R^*\|M)$.

2. Сравнить значение E и E^*. Если $E = E^*$, то подпись к сообщению M признаётся подлинной.

4. Реализация схемы слепой цифровой подписи

Протокол слепой ЭЦП характеризуется тем, что субъект, подписывающий электронное сообщение M, приготовленное некоторым другим субъектом (запрашивающим), не должен знать содержания сообщения M, и позже, после процедуры генерации ЭЦП подписывающий не сможет установить связь между подписанным сообщением и его автором. Схема ЭЦП, описанная в разделе 3, положена в основу следующего протокола слепой ЭЦП.

1. Подписывающий генерирует случайное 256-битное число k и вычисляет $R^* = \alpha^k \bmod n$, затем отправляет R^* запрашивающему.

2. Запрашивающий генерирует два случайных 256-битных числа ε и μ (которые называются «маскирующими» параметрами) и вычисляет $R = R^* y^{\mu}\alpha^{\varepsilon} \bmod n$. Затем используя 256-битную хэш-функцию F_H, он вычисляет $H = F_H(M)$ и $E = F_H(R\|M)$, и $E^* = E + \mu \bmod \gamma$. Значение E – первый элемент подписи к документу M, а E^* является первым элементом слепой подписи. Запрашивающий отправляет E^* подписывающему.

3. Подписывающий вычисляет второй элемент слепой подписи: $S^* = (k + xE^*) \bmod \gamma$, затем отправляет S^* запрашивающему.

4. Запрашивающий «демаскирует» параметр S^*, то есть вычисляет второй элемент подписи (E,S) к сообщению $M: S = S^* + \varepsilon \bmod \gamma$.

Процедура проверки слепой подписи выполняется по алгоритму проверки обычной ЭЦП, описанной в разделе 3.

5. Реализация протокола с нулевым разглашением

Используя сложность ЗДЛ по трудно разложимому модулю и открытые ключи вида (n,α,y), можно предложить следующий протокол:

1. Проверяющий генерирует случайное число $k < \gamma$ и вычисляет значения $U = \alpha^k \bmod n$ и $Z = \alpha^k \bmod n$ где y, n и α – элементы открытого ключа доказывающего (пользователя, подлинность которого проверяется), после чего передает доказывающему значение U в качестве своего запроса.

2. Доказывающий проверяет выполнимость соотношения $U^{\gamma} \bmod n = 1$. Если это соотношение выполняется, то он вычисляет значение $Z^* = U^x \bmod n$ и направляет Z^* проверяющему в качестве своего ответа на полученный запрос. В противном случае направляется ответ «Некорректный запрос».

Если $Z^* = Z$, то проверяющий делает вывод о подлинности доказывающего. Нулевая утечка информации обеспечивается тем, что проверяющий получает ответ, который он вычисляет самостоятельно на первом шаге, т.е. до того как это значение вычислено доказывающим. Проверка на втором шаге порядка числа U является принципиальным моментом. Если эта проверка не делается, то проверяющий может в качестве запроса U выбирать случайные числа (в этом случае вероятность выполнимости соотношения $U^{\gamma} \bmod = 1$ является пренебрежимо малой) и в качестве

ответа получать значения, которые ему не были заранее известны, т.е. в этом случае нельзя говорить о нулевой утечке информации о секрете.

6. Реализация протокола открытого распределения ключей

Предполагается, что каждый i-й пользователь (i=1,2,3,…) генерирует секретные простые значения p_i, q_i, и случайное 256-битное число x_i. Затем, он вычисляет свой открытый ключ (n_i, α_i, y_i), где $n_i = p_i q_i;\ \ y_i = \alpha_i^{x_i} \bmod n_i; \alpha_i$ имеет 256-битовый простой порядок по модулю n_i. Открытый ключ (n_i, α_i, y_i) регистрируется в удостоверяющем центре, который публикует все открытые ключи пользователей в каталоге. Пользователи i и j могут вычислить их общий секретный ключ Z_{ij}, используя следующий протокол:

1. Пользователь i генерирует случайное 256-битное число u_i, вычисляет значение $R_i = \alpha_j^{u_i} \bmod n_j$, и отправляет R_i пользователю j.

2. Пользователь j генерирует случайное 256-битное число u_j, вычисляет значение $R_j = \alpha_i^{u_j} \bmod n_i$, и отправляет R_j пользователю i.

3. Пользователь i берёт из каталога открытый ключ y_j и вычисляет следующие значения $Z_{ij}^{'} = y_j^{u_i} \bmod n_j$, $Z_{ij}^{''} = R_j^{x_i} \bmod n_i$ и $Z_{ij} = Z_{ij}^{'} Z_{ij}^{''}$.

4. Пользователь j берёт из каталога открытый ключ y_i и вычисляет следующие значения $Z_{ji}^{'} = y_i^{u_j} \bmod n_j$, $Z_{ji}^{''} = R_i^{x_j} \bmod n_j$, и $Z_{ji} = Z_{ji}^{'} Z_{ji}^{''}$.

Секретный ключ, полученный обоими пользователями, одинаков $Z_{ji} = Z_{ij}$.

7. Реализация протоколов открытого и коммутативного шифрования

Пусть кто-то хочет отправить сообщение $M < n$ некоторому пользователю по открытому каналу связи. Это может быть произведено с помощью следующего алгоритма открытого шифрования, аналогичного алгоритму шифрования Эль-Гамаля [1].

1. Отправитель берёт открытый ключ получателя (n, α, y) из каталога, генерирует случайное 256-битное число u, вычисляет $R = \alpha^u \bmod n$, и $Z = y^u \bmod n$.

2. Затем шифрует сообщение M по формуле: $C = MZ \bmod n$.

3. Отправляет криптограмму (R, C) получателю.

Процедура расшифровки сообщения M:

1. Получатель, используя свой секретный ключ x такой, что $y = \alpha^x \bmod n$, вычисляет значение $W = R^{-x} \bmod n$.

2. Затем восстанавливает сообщение $M : M = CW \bmod n$.

3. Данный подход применим для построения протокола коммутативного шифрования в том случае, когда используется несоставной порядок γ, известный всем пользователям.

Пусть требуется зашифровать сообщение длины меньше n.

1. Сгенерируем случайное число $k < \gamma$ и вычислим значение $K = \alpha^k \bmod n$. Разобьём сообщение M в зависимости от K по модулю n, например, по формуле $C = (M + K)K \bmod n$. Сообщение M можно легко восстановить из пары значений (C, K), поэтому можно говорить о расщеплении сообщения M на два значения C и K, причем C – число произвольного вида, а число K принадлежит множеству значений $\{\alpha^1 \bmod n, \alpha^2 \bmod n, ..., \alpha^\gamma \bmod n\}$.

2. Зашифруем значение $K : S = K^e \bmod n$. На выходе первичной процедуры шифрования имеем пару значений (C, S).

3. Последующие шаги зашифрования/расшифрования выполняются над значением S.

4. Завершающий шаг расшифрования выполняется как расшифрование значения S, приводящее к восстановлению значения K, выбранного на шаге первичного шифрования сообщения, и вычисление значения M по формуле $M = CK^{-1} - K \bmod n$.

Данный алгоритм позволяет выполнять шифрование сообщений произвольного вида.

Заключение

В работе показана конструктивная эффективность предложенного подхода. С его использованием возможно построение криптосхем, обладающих одинаковой стойкостью ЗФ и ЗДЛ, что позволяет гарантировать общую стойкость криптосхемы на одном уровне (т.е. стойкость такой криптосхемы не изменится в случае открытия прорывного алгоритма для решения одной из рассматриваемых задач). Данный подход является интересным и достаточно универсальным для построения криптосхем различных типов, основанных на трудности одновременного решения ЗФ и ЗДЛ. При его применении к существующим криптосхемам потребуется минимальная их модификация. При этом производительность понизится всего лишь в 2.25 раза по сравнению с базовыми криптосхемами [7]. В случае построения схем ЭЦП, возможно достижение 128 битовой стойкости при размере подписи в 512 и даже 384 бита, что существенно меньше размеров известных схем ЭЦП.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2005, 286 с.
2. Minh N.H., Binh D.V., Giang N.T., Moldovyan N.A. Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems // Applied Mathematical Sciences. 2012, V.6, №139, P.6903–6910.
3. Tahat N.M.F., Shatnawi S.M.A., Ismail E.S.: A New Partially Blind Signature Based on Factoring and Discrete Logarithms // J.of Mathematics and Statistics. 2008, V.4 (2), P.124–129.
4. N.M.F. Tahat, E.S. Ismail and R.R. Ahmad, A New Blind Signature Scheme Based On Factoring and Discrete Logarithms, International Journal of Cryptology Research. 2009, V.1 (1), P.1 – 9.
5. Menezes A.J., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1996, 780p.
6. Moldovyan A.A., Moldovyan D.N., Gortinskaya L.V. Cryptoschemes based on new signature formation mechanism // Computer Science Journal of Moldova. 2006, V.14, №3 (42). P.397–411.
7. Berezin A.N., Moldovyan N.A., Shcherbacov V.A. Cryptoschemes Based on Difficulty of Simultaneous Two Different Difficult Problems // Computer Science Journal of Moldova. 2013, V.21, №2 (62), P.280–290.
8. Березин А.Н., Молдовян Н.А., Латышев Д.М. Протокол 240–битовой коллективной подписи над нециклической конечной группой // Вопросы защиты информации. 2013, №3, С.81–85.
9. Schnorr C.P. Efficient signature generation by smart cards // Journal of Cryptology. 1991, V.4, P.161–174.

УДК 681.3

ПРОТОКОЛЫ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, ИСПОЛЬЗУЮЩИЕ АЛГОРИТМЫ ОТКРЫТОГО ШИФРОВАНИЯ

Березин Андрей Николаевич, Демьянчук Анна Алексеевна, Рыжков Алексей Викторович,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профеесора Попова, д. 5,
e-mails: a.n.berezin.ru@gmail.com, vleti@yandex.ru, ryzhkov.alex@gmail.com.

Аннотация: В работе предложен новый подход к построению протоколов с нулевым разглашением. В его основе лежит использование специфицированных меток вместо хэш-функций, что приводит к упрощению протоколов. Предложены конкретные варианты реализации протоколов с нулевым разглашением на основе алгоритмов открытого шифрования, RSA, Эль-Гамаля, Рабина. Рассмотрены варианты вычислительно эффективной реализации с использованием вычислений в поле двоичных многочленов, порядок которых равен степеням Мерсенна. Предложенные механизмы повышают быстродействия протоколов аутентификации, при этом гарантируют, что никакие запросы со стороны проверяющего не могут быть использованы для получения информации о ключе.

Ключевые слова: п*ротоколы с нулевым разглашением; степени Мерсенна; простые числа Мерсенна; криптосхемы с открытым ключом*

ZERO KNOWLEDGE PROTOCOLS BASED ON THE PUBLIC ENCRYPTION ALGORITHMS

Berezin Andrey, Dem'janchuk Anna, Rizhkov Aleksey,
The St-Petersburg State Electrotechnical University «LETI»,
Russia, St-Petersburg, Professor Popov str. 5,
e-mails: a.n.berezin.ru@gmail.com, vleti@yandex.ru, ryzhkov.alex@gmail.com.

Annotation: There is proposed a new approach to constructing zero-knowledge protocols, which is characterized in using specified labels instead of using the hash-functions. The approach provides simplification of the protocol. Some implementations of the zero-knowledge protocols, which use the RSA, ElGamal, and Rabin public encryption algorithms, are considered. There is also considered computationally efficient implementation of the protocol using computations in the finite fields of the binary polynomials.

Key words: *zero knowledge protocols; Mersenne exponents; Mersenne primes; public key cryptoschemes.*

Введение

Протоколы с нулевым разглашением секрета (без разглашения секрета) относятся к двухключевым криптосистемам и применяются для аутентификации удаленных абонентов информационно-телекоммуникационных систем. Интерпретация термина «нулевое разглашение секрета» отражена в работе [1]. Рассмотрим основные моменты:

1. В протоколах присутствует некоторая начальная утечка информации о личном секретном ключе пользователя (ЛСК), которая предоставляет потенциальную возможность вычислить ЛСК по открытому ключу пользователя (ОК).
2. Начальная утечка информации о ЛСК считается допустимой, так как вычисление ЛСК по ОК является вычислительно трудной задачей и практически нереализуемо; вычислительная трудность этой задачи определяет стойкость протокола.
3. Под нулевой утечкой информации о ЛСК подразумевается, что при выполнении протокола не происходит дополнительной утечки информации о секрете.
4. В ходе протокола отсутствуют какие-либо дополнительные разглашения секрета, так как формируемые и передаваемые по каналам связи наборы случайных значений могут быть выработаны без знания секрета, то есть без использования ЛСК.

В протоколах с нулевым разглашением используется многораундовая процедура [2], [3], каждый раунд которой состоит из трех следующих шагов:

1. Доказывающий (субъект, который доказывает свою подлинность в ходе протокола) генерирует разовый случайный секретный ключ, вычисляет по нему разовый ОК (фиксатор) и направляет последний проверяющему, т.е. пользователю, желающему убедиться в том, что доказывающий знает ЛСК, связанный с ОК.
2. После получения разового ОК проверяющий генерирует запрос в виде случайного бита e и посылает его доказывающему.
3. В зависимости от полученного значения $e \in \{0,1\}$ доказывающий вычисляет ответ, который направляется проверяющему.

В каждом раунде подлинный доказывающий даёт правильный ответ с вероятностью равной единице, а нарушитель – с вероятностью 0,5. При увеличении количества раундов можно снизить вероятность обмана до приемлемо низкой величины. Однако, в случае использования вычислительно трудных задач некоторых типов за счёт использования массива ОК (вместо одного ОК), возможно построение однораундового протокола. Актуальной представляется задача уменьшения размера используемого ОК и количества раундов, при обеспечении достаточной очевидности отсутствия передачи информации о личном секретном ключе в ходе выполнения протокола.

В данном сообщении рассматривается подход к построению протоколов с нулевым разглашением, основанный на идее использования алгоритмов открытого шифрования в качестве основного механизма протокола, по аналогии с двухшаговыми протоколами, описанными в стандарте ISO/IEC 9798-5:2009(E) [4], и отличается от последних использованием специфицированных меток вместо хэш-кодов. При этом в ходе протокола не происходит никакой утечки информации о ЛСК.

1. Структура протоколов с нулевым разглашением, использующих алгоритмы открытого шифрования

В протоколах такого типа используется некоторый алгоритм открытого шифрования $Publ_Encr$. Проверяющий может направить доказывающему некоторое случайное сообщение M, предварительно зашифровав его по открытому ключу (ОК) доказывающего, т.е. направив доказывающему криптограмму $C = Publ_Encr(M, P)$, где P – открытый ключ доказывающего. Прочитать это сообщение сможет только хозяин ЛСК, связанного с ОК, то есть подлинный доказывающий. После получения значения C в качестве случайного запроса, доказывающий должен расшифровать криптограмму и направить проверяющему ответ в виде исходного сообщения M, таким образом, проверяющий получает уже известное ему значение. Поскольку проверяющий получил значение которое уже знает, то утечки информации о ЛСК доказывающего не происходит. При этом проверяющий получает информацию о том, что доказывающий является подлинным.

При разработке конкретных протоколов с нулевым разглашением на основе рассмотренного подхода следует учитывать особенности используемых алгоритмов открытого шифрования. Важной особенностью является однозначность результата расшифрования криптограммы, при которой доказывающий вычисляет для своего ответа то же самое значение M, которое было использовано проверяющим для формирования своего запроса. Например, при использовании способа открытого шифрования Рабина результат расшифрования неоднозначен, поэтому для его применения при синтезе протоколов с нулевым разглашением требует использования дополнительного механизма, для обеспечения распознавания доказывающим значения M, известного проверяющему.

Однако следует учитывать и то, что проверяющий имеет возможность выбрать случайный запрос, а не формировать его как криптограмму, полученную с помощью процедуры открытого шифрования. В этом случае проверяющий не знает заранее ответа на свой запрос, а следовательно нужно считать, что он получает некоторую информацию о секретном ключе, т.е. он может как-то использовать эту возможность для раскрытия ЛСК доказывающего. В стандарте [4] роль такого механизма исполняет некоторая хэш-функция h для вычисления хэш-кода от сообщения H, и формирования запроса как криптограммы, полученной путём шифрования сообщения M с присоединённым к нему значением h.

В предлагаемых двухшаговых протоколах с нулевым разглашением используется механизм включения заранее специфицированных меток μ в исходное сообщение, которое шифруется проверяющим. Наличие такой метки в сообщении, расшифрованном доказывающим, показывает, что запрос был сформирован корректно. Размер меток $|\mu|$ выбирается равным от 80 до 512 бит, благодаря чему вероятность P того, что расшифрование некорректно сформированного запроса даст текст, в котором будет присутствовать метка является пренебрежимо малой $(P = 2^{-|\mu|})$. Использование меток устраняет необходимость дополнительного использования хэш-функций и выполнения вычисления хэш-кода как проверяющим, так и доказывающим.

2. Протокол на основе алгоритма шифрования подобного RSA

Рассмотрим случай построения протокола с нулевым разглашением с использованием алгоритма открытого шифрования RSA [5]. Значения соответствующих друг другу ЛСК и ОК формируются пользователем следующим путем. Выбираются два больших не равных между собой сильных простых числа r и q [6], вычисляется произведение $n = rq$ и значение обобщенной функции Эйлера $L(n)$ от числа n, равное наименьшему общему кратному чисел $r-1$ и $q-1$. После этого генерируется случайное 32-битовое число e, взаимно простое с $L(n)$ и вычисляется число d, удовлетворяющее условию

$$ed \equiv 1 \bmod L(n).$$

Пара значений n и e является открытым ключом. Тройка чисел r, q и d является личным секретным ключом пользователя. Числа r и q должны иметь специальную структуру, в частности, они должны иметь разрядность не менее 512 бит и каждое из чисел $r-1$ и $q-1$ должно содержать в своем разложении один большой простой множитель. Процедура открытого шифрования сообщения $M < n$ описывается формулой

$$C = M^e \bmod n.$$

Процедура расшифрования криптограммы C описывается формулой

$$M = C^d \bmod n.$$

Корректность процедуры расшифрования легко доказывается с использованием обобщенной теоремы Эйлера, согласно которой для любого числа M, взаимно простого с n имеет место соотношение

$$M^{L(n)} \equiv 1 \bmod n.$$

Двухпроходный протокол с нулевым разглашением на основе данного алгоритма открытого шифрования использует 256-битовую метку μ, в качестве которой берутся младшие 256 бит итерационной константы C_2 из стандарта ГОСТ Р 34.11-2012 (т.е. специфицируется $\mu = C_2 \bmod 2^{256}$) и описывается следующими шагами:

1. Проверяющий генерирует случайное сообщение M размером $|M|$, удовлетворяющим условию $|n|/2 < |M| < |n| - |\mu|$. Затем он зашифровывает сообщение M с присоединенной к нему меткой μ, т.е. зашифровывает битовую строку $M \| \mu$ по ОК доказывающего (n, e), т.е. по формуле $C = (M \| \mu)^e \bmod n$ и направляет доказывающему значение C в качестве своего запроса, на который он ожидает ответ доказывающего.

2. Доказывающий расшифровывает криптограмму C по своему личному секретному ключу d по формуле $M \| \mu = C^d \bmod n$, где μ'-битовая строка, заданная младшими 256 битами расшифрованного значения, и проверяет выполнимость равенства $\mu' = \mu$. Если $\mu' = \mu$, то

полученное значение M' доказывающий направляет проверяющему в качестве своего ответа на полученный запрос. В противном случае доказывающий отправляет ответ «Некорректный запрос».

Если проверяющий получил правильное значение $M' = M$, т.е. то значение, которое он сгенерировал на первом шаге протокола, т.е. до направления своего запроса доказывающему, то им делается вывод о подлинности доказывающего.

В описанном протоколе важным является использование заранее специфицированной метки μ, благодаря чему обеспечивается возможность доказывающему удостовериться в том, что отправляемое им значение M' уже известно проверяющему. Тот факт, что оно уже известно проверяющему, означает, что проверяющий не пытается получить подпись проверяющего к некоторому сообщению, используя механизм слепой подписи [7[, [8], и не пытается выполнить атаку при адаптивно выбираемом шифртексте (adaptive chosen cipher text attack), описанную в работе [9] или какую-то другую атаку.

3. Протокол на основе алгоритма шифрования подобного Эль-Гамаля

Рассмотрим реализацию прокола с использованием алгоритма открытого шифрования Эль-Гамаля [10]. В способе открытого шифрования Эль-Гамаля используются ОК вида $y = \alpha^x \bmod p$, где p – большое простое число (размером 1024 бит и более), такое, что разложение числа $p-1$ содержит простой делитель разрядностью не менее 160 бит; α – примитивный элемент по модулю p. Этот способ фактически представляет собой гибридную криптосистему, в которой секретные ключи распределяются в соответствии с протоколом Диффи–Хеллмана [11], а шифрование сообщения выполняется путем модульного умножения сообщения на секретный ключ. Шифрование сообщения T, отправляемого владельцу ОК y, осуществляется с помощью следующего алгоритма:

1. Сгенерировать случайное число k, которое по своей сути является разовым ЛСК.
2. Вычислить число $R = \alpha^k \bmod p$ – разовый ОК отправителя.
3. Используя ОК получателя y, вычислить разовый общий секретный ключ $Q = y^k \bmod p$.
4. Зашифровать сообщение M путем умножения сообщения на разовый секретный ключ: $C = QM \bmod p$.
5. Отправить получателю криптограмму в виде пары чисел (R, C).
6. Процедуру открытого шифрования по ОК y обозначим как $Gamal_Encr(M, y)$.

Получатель криптограммы (R, C), используя свой ЛСК x, выполняет процедуру расшифрования $Gamal_Decr(R, C, x)$, которая описывается следующими шагами:

1. Вычислить разовый общий секретный ключ $Q = R^x \bmod p$.
2. Используя расширенный алгоритм Евклида, вычислить значение Q^{-1}, обратное значению Q по модулю p.
3. Расшифровать сообщение M путем умножения значения C на целое число $Q^{-1}: M = CQ^{-1} \bmod p$.

При зашифровании сообщений в алгоритме Эль-Гамаля используются случайные значения, т.е. он реализует процедуру вероятностного шифрования, при котором одному и тому же сообщению соответствует множество различных криптограмм, все из которых при расшифровании дают одно и то же выходное значение M.

Предлагаемый протокол аутентификации с нулевым разглашением на основе алгоритма Эль-Гамаля использует 128-битовую метку μ, в качестве которой берутся младшие 128 бит итерационной константы C_3 из стандарта ГОСТ Р 34.11–2012 (т.е. специфицируется $\mu = C_3 \bmod 2^{128}$) и описывается следующим образом:

1. Проверяющий генерирует случайное сообщение M размером $|M|$, удовлетворяющим условию $|p|/2 < |M| < |p| - |\mu|$. Затем он зашифровывает сообщение M с присоединенной к нему меткой μ, т.е. зашифровывает битовую строку $M \| \mu$, по ОК доказывающего y в соответствии с формулой $(R, C) = Gamal_Encr(M \| m, y)$. Затем он направляет доказывающему пару (R, C) в качестве своего запроса, на который должен дать ответ доказывающий.

2. Доказывающий расшифровывает криптограмму (R,C) по своему ЛСК $x: M'\|\mu = Gamal_Decr(R,C,x)$, где μ' – битовая строка, заданная младшими 128 битами расшифрованного значения, и проверяет выполнимость равенства $\mu' = \mu$. Если $\mu' = \mu$, то полученное значение M' доказывающий направляет проверяющему в качестве своего ответа на полученный запрос. В противном случае доказывающий отправляет ответ «Некорректный запрос».

Если проверяющий не имеет своей целью получение информации о ЛСК доказывающего, то он корректно выполняет первый шаг протокола с использованием специфицированной метки μ, присоединяемой к выбираемому им сообщению M и получает в качестве ответа на свой запрос значение $M' = M$, т.е. получает известное ему значение и делает вывод о подлинности доказывающего. Вероятность выполнения соотношения $\mu' = \mu$ для произвольно выбранного проверяющим запроса, направляемого доказывающему для расшифрования (т.е. при некорректных действиях проверяющего на первом шаге протокола, когда он не знает расшифрованного текста) пренебрежимо мала (равна $2^{-|\mu|}$).

4. Протокол на основе способа открытого шифрования Рабина

В алгоритме открытого шифрования Рабина [3], [12] используются вычисления по трудно разложимому модулю вида $n = pq$, который представляет собой ОК. Сильные простые числа p и q составляют ЛСК и сравнимы с числом 3 по модулю 4: $p \equiv 3 \bmod 4$ и $q \equiv 3 \bmod 4$. Последнее условие обеспечивает владельцу ОК, который знает соответствующий ему ЛСК, снижение сложности операции извлечения квадратного корня из квадратичных вычетов по модулю n, выполнение которой требуется при расшифровании криптограммы.

Зашифрование сообщения $M < n$ выполняется путем возведения числа M в квадрат по модулю n (по ОК)

$$C = M^2 \bmod n.$$

Процедура расшифрования состоит в извлечении квадратного корня из криптограммы C по модулю n. Предварительно вычисляют корни из C по модулям p и q:

$$m_{p_1} = C^{\frac{p+1}{4}} \bmod p,\ m_{p_2} = p - m_{p_1} = p - C^{\frac{p+1}{4}} \bmod p;$$

$$m_{q_1} = C^{\frac{q+1}{4}} \bmod q,\ m_{q_2} = q - m_{q_1} = q - C^{\frac{q+1}{4}} \bmod q.$$

Из этих четырех значений вычисляются четыре возможных корня из C по модулю n:

$$M_1 = (m_{p_1} a + m_{q_1} b) \bmod n,$$
$$M_2 = (m_{p_1} a + m_{q_2} b) \bmod n,$$
$$M_3 = (m_{p_2} a + m_{q_1} b) \bmod n,$$
$$M_4 = (m_{p_2} a + m_{q_2} b) \bmod n,$$

где $a = q(q^{-1} \bmod p)$ и $b = p(p^{-1} \bmod q)$.

Двухпроходный протокол с нулевым разглашением на основе алгоритма открытого шифрования Рабина использует 512-битовую метку μ, в качестве которой берется итерационная константа C_1 из стандарта ГОСТ Р 34.11–2012 (т.е. $\mu = C_1$), и имеет следующий вид:

1. Проверяющий генерирует произвольное сообщение M размером $|M|$, удовлетворяющим условию $|n|/4 < |M| < |n| - |\mu|$, и зашифровывает сообщение M с присоединенной к нему меткой μ, т.е. значение $M\|\mu$, по формуле $C = (M\|\mu)^2 \bmod n$ и направляет доказывающему значение C в качестве своего запроса, на который он ожидает ответ доказывающего.

2. Доказывающий расшифровывает криптограмму C по своему ЛСК (p,q)) путем вычисления четырех значений квадратного корня из $C: M_1, M_2, M_3, M_4$. Каждое из последних значений он представляет в виде $M'_i\|\mu'_i$, где μ' – битовая строка, заданная младшими 512 битами i-го корня $(i = 1,2,3,4)$. Затем он проверяет, выполняется ли равенства $\mu' = \mu$ для одного из четырех значений i.

Если выполняется, то соответствующее значение M'_i доказывающий направляет проверяющему в качестве своего ответа на полученный запрос. Если $\mu' \neq \mu$ для $i = 1,2,3,4$, то доказывающий отправляет ответ «Некорректный запрос».

Использование заранее специфицированной метки позволяет доказывающему идентифицировать исходное сообщение, благодаря чему он направляет проверяющему именно то значение, которое известно проверяющему. Это обеспечивает нулевую утечку информации о ЛСК при передаче доказывающим своего ответа проверяющему. По аналогии с описанным в этом разделе протоколом можно разработать протоколы с нулевым разглашением, основанные на криптосхемах, описанных в работе [13] и представляющих собой класс алгоритмов открытого шифрования с неоднозначным расшифрованием криптограммы.

5. Вопросы реализации протоколов

Наиболее эффективная реализация протоколов такого типа связана с использованием поля двоичных многочленов $GF(2^s)$, порядок мультипликативной группы q которых равен простому числу вида $2^s - 1$ (числа Мерсенна). Числа такого вида являются простыми, только при определенных значениях s. Практический интерес для реализации протокола с нулевым разглашением представляют следующие шесть значений степеней Мерсенна: 1279, 2203, 2281, 3217, 4253, 4423, поскольку при их использовании достигается приемлемый компромисс между стойкостью и производительностью.

Примерами неприводимых двоичных многочленов таких степеней являются:

$x^{1279} + x^{216} + 1, x^{1279} + x^{418} + 1$, $x^{2203} + x^{14} + x^{6} + x^{5} + 1$, $x^{2281} + x^{715} + 1$, $x^{2281} + x^{915} + 1$, $x^{2281} + x^{1029} + 1$, $x^{3217} + x^{67} + 1$, $x^{3217} + x^{576} + 1$, $x^{4253} + x^{21} + x^{12} + x^{11} + 1$, $x^{4423} + x^{271} + 1$, $x^{4423} + x^{369} + 1$.

При выборе указанных трёхчленов в качестве модуля, операция модульного умножения двоичных многочленов в поле может быть выполнена путем осуществления одной операции арифметического умножения многочленов, двух операций арифметического сдвига и шести операций сложения. Выполнение операции деления многочленов не требуется, что существенно снижает сложность вычислений в поле $GF(2^s)$ и повышает быстродействие протокола аутентификации. Для некоторых степеней Мерсенна не существует неприводимых двоичных трёхчленов, В этом случае умножение в поле $GF(2^s)$ может быть задано по модулю неприводимого пятичлена. При этом умножение можно выполнить без осуществления операции деления многочленов, путём осуществления одной операции арифметического умножения многочленов, шести операций арифметического сдвига и десяти операций сложения. В этом варианте протокола нет необходимости выполнять проверку корректности запроса, поскольку любая ненулевая битовая строка, интерпретируемая как элемент поля $GF(2^s)$, имеет порядок равный простому числу Мерсенна, т.е. никакие запросы со стороны проверяющего не могут быть им использованы для получения хотя бы одного бита информации о ключе.

Заключение

Предложенный подход к построению двухпроходных протоколов аутентификации с нулевым разглашением отличается от протоколов, описанных в стандарте [4], включением в сообщение, шифруемое по ОК доказывающего, специфицированных меток. Это позволяет отказаться от использования хэш-функций, что приводит к упрощению протокола вследствие исключения процедуры вычисления хэш-кодов. Предложены конкретные варианты протоколов, построенные в рамках данного подхода. Нулевая утечка информации о секретном ключе обеспечивается тем, что ответ, отправляемый доказывающим, уже известен проверяющему, что гарантируется наличием специфицированных меток в расшифрованном значении. Размер меток от 80 бит обеспечивает приемлемо низкую вероятность того, что расшифрование некорректно сформированного запроса даст текст, в котором будет присутствовать метка.

Рассмотрен вариант эффективной реализации предложенных протоколов с использованием вычислений в поле двоичных многочленов, порядок которых равен степеням Мерсенна. При выборе в качестве модуля двоичных трёхчленов или пятичленов со степенями равными числам Мерсенна, при выполнении модульного умножения многочленов в поле, операция деления многочленов не требуется, что существенно снижает сложность вычислений, и, следовательно повышает быстродействие протоколов аутентификации, при этом гарантируя, что никакие запросы со стороны проверяющего не могут быть использованы для получения информации о ключе.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян А.А., Молдовян Д.Н., Васильев И.Н., Головачев Д.А. Протоколы с нулевым разглашением секрета и обоснование безопасности схем цифровой подписи // Вопросы защиты информации. 2011, №4, С.6–11.
2. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in cryptology – CRYPTO'86, Springer-Verlag LNCS, 1987, Vol. 263, P.186–194.
3. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Санкт-Петербург, БХВ–Петербург, 2005, 286 с.
4. ISO/IEC 9798-5:2009(E) «Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques».
5. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001, 323с.
6. Gordon J. Strong primes are easy to find // Advances in cryptology – EUROCRYPT'84. Springer-Verlag LNCS. 1985, Vol.209, P.216–223.
7. Chaum D. Blind Signatures for Untraceable Payments // Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983, P.199–203.
8. Pieprzyk J., HardjonoTh., Seberry J. Fundumentals of Computer Security. Springer-verlag. Berlin, 2003, 677p.
9. Bleichenbacher D. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1 // Advances in Cryptology – CRYPTO'98. Springer-Verlag LNCS. 1998. Vol.1462, P.1–12.
10. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985, Vol. IT-31, №4, P.469–472
11. Diffie W., Hellman M.E. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976, Vol. IT-22, P.644–654.
12. Rabin M.O. Digitalized signatures and public key functions as intractable as factorization. – Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.
13. Moldovyan N.A., Moldovyan A.A. Class of Provably Secure Information Authentication Systems // 4th Int. Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS'07 Proc. September 13–15, 2007 / Springer Verlag CCIS. 2007 Vol.1, P.147–152.

УДК 681.3

ОТКАЗОУСТОЙЧИВОСТЬ КОНФИГУРАЦИЙ ЦЕНТРОВ ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ

Богатырев Владимир Анатольевич[1], Богатырев Анатолий Владимирович[2],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, д. 49,
e-mail: vladimir.bogatyrev@gmail.com

Аннотация: Исследуется отказоустойчивость и надежность конфигураций кластеров с прямым подключением устройств хранения к дублированным серверам приложений m типов, в которых каждый сервер имеет два порта (входа) для подключения устройств хранения, а каждое устройство хранения два входа для подключения серверов.

Ключевые слова: *отказоустойчивость; кластер; надежность; сервер; система хранения; сеть хранения; резервирование; конфигурация кластера; подключение системы хранения к серверу.*

FAILOVER CONFIGURATION DATA CENTERS

Bogatyrev Vladimir [1], Bogatyrev Anatoly [2],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
[2]St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverkskiy av. 49,
e-mail: vladimir.bogatyrev@gmail.com.

Abstract: Investigate the availability and reliability of cluster configurations direct attached storage to a redundant application servers m types, where each server has two ports (input) for connection of storage devices, and each device storage two inputs for connecting servers.

Keywords: *fault tolerance; clustering; security; server; storage; network storage; redundancy; cluster configuration; connect the storage system to the server.*

Введение. К центрам хранения и обработки данных предъявляются повышенные требования по информационной безопасности надежности, отказоустойчивости, доступности [1-5]

Базовым решением при построении защищенных центров хранения и обработки данных в настоящее время является использование систем кластерной архитектуры, обладающих высокой отказоустойчивостью (Fault Tolerance), доступностью (Availability), надежностью (Reliability) и производительностью приложений.

Высокая доступность (High Availability) кластеров (cluster) достигается в результате, консолидации устройствам хранения (Storage), при которой каждый вычислительный узел – сервер (Server) кластера имеет доступ ко всем информационным ресурсам [2],[3]. В крупномасштабных

системах консолидация устройств хранения достигается на основе технологии сетей хранения данных Storage Area Network (SAN) - сетей, предназначенных для обеспечения подключения вычислительных узлов (серверов) к устройствам хранения (к дискам, RAID-массивам - Redundant Array of Independent Disks - и ленточным библиотекам) и обмена данными между ними [2].

Сети хранения выдвигают жесткие требования к надежности и производительности коммутаторов (Switch) и маршрутизаторов. Узлы, подключенные к SAN, предназначены для прямой связи с устройствами хранения, поэтому доставка с нарушением порядка пакетов или их потери должны быть исключены [2].

Коммутационные узлы, обеспечивающие требования сетей хранения, характеризуются высокой стоимостью и сложностью, что может в ряде случаев отрицательно влиять на эффективность и надежность кластерных систем. В связи с этим при построении не больших кластерных систем в ряде случаев целесообразно прямое подключение устройств хранения к серверным (вычислительным) узлам (архитектура DAS- Directly Attached Storage) [2].

Типовой вариант построения кластера с дублированием устройств хранения и их прямым подключением к дублированным серверам (архитектуры DAS), описанный в работе [2] представлен на рисунке1. В конфигурации по рисунку 1 выделяются группы, содержащие пару серверов и пару устройств хранения при их полной связанности между собой.

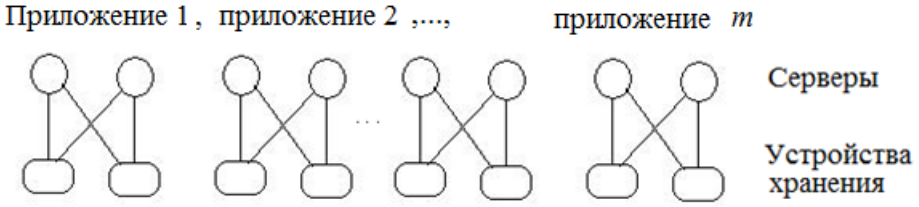


Рис. 1. Типовой вариант построения кластера с прямым подключением устройств хранения

В случае *m* типов приложений (функций) и выделения каждой из m групп дублированных серверов для работы с определенным типом приложений будем считать, что работоспособность системы обеспечивается при исправности в каждом из m групп хотя бы одного сервера и хотя бы одного устройства хранения.

Представляет определенный интерес дополнительное исследование вариантов построения кластеров с прямым подключением серверов к устройствам хранения. Цель таких исследований - обосновать выбор конфигураций, обеспечивающих при одинаковых затратах на реализацию системы ее большую отказоустойчивость надежность и доступность [5].

Под работоспособным состоянием кластера подразумевается его состояние при доступности серверов приложений всех типов (хотя бы по одному каждого типа) и условии доступности для каждого типа серверов приложений хотя бы одного устройства хранения.

Сложность предполагаемых исследований обусловлено тем, что в общем случае модели надежности рассматриваемых конфигураций, не сводятся к параллельно-последовательным или иным известным моделям надежности позволяющим учесть комбинаторное влияния расположения отказов узлов на отказоустойчивость системы при различных вариантах прямой связанности серверов и устройств хранения.

Исследуемые системы при выполнении в них *m* приложений могут рассматриваться как многофункциональные, однако модели надежности многофункциональных систем, описанные в работах [6-9], не позволяют учесть особенности комбинаторного влияния отказов на устойчивость исследуемых конфигураций.

2. Варианты построения кластера. Рассмотрим конфигурации кластерных систем с непосредственным подключением устройств хранения к серверам приложений m типов.

Будем считать, что запрос к i- му приложению может быть обслужен только сервером i- го типа, при его взаимодействии с любым из подключенных к нему устройств хранения. Взаимодействие сервера с устройством хранения происходит только во время решения задачи, при этом не требуется данных, сформированных в результате предыдущих выполнений приложения.

Кратность резервирования серверов приложений будем считать 2/1 (дублирование), в этом случае общее число серверов 2m, общее число устройств хранения будем считать также равным 2m. Емкость каждого устройства хранения достаточна для поддержки функционирования двух типов приложений.

В работоспособном состоянии система (кластер) должна обеспечить доступность к серверам приложений каждого из m типов, при условии доступности для этих серверов хотя бы одного устройства хранения на время решения запрашиваемой задачи.

При формировании структур рассмотрим случай, когда каждый сервер имеет два порта (входа) для подключения устройств хранения, а каждое устройство хранения два входа для подключения серверов (a=2), что дает возможность строить резервированные системы без использования коммутаторов, которые в ряде случаев могут вносить дополнительную ненадежность в систему.

При анализе отказоустойчивости предположим, что любой отказ сервера или устройства хранения приводит к потере их функциональности (к их полному отказу). Требуется дополнительно к конфигурации кластера по рис 1 сформировать варианты его построения и проанализировать их отказоустойчивость.

Рассмотрим варианты конфигурации кластера с непосредственным подключением устройств хранения к серверам, которые охарактеризуем вектором (l,s,r,m), где m-число типов серверов приложений, r – кратность их резервирования (при дублировании r=2) l число типов серверов приложения объединяемых в группы, s смещение при связи сервера и устройства хранения в группе.

При заданных l и s варианты конфигурации формируются по следующему правилу: в каждой группе первый сервер подключен к первому входу первого и ко второму входу s-го устройства хранения, i-й сервер подключен к первому входу i-го и ко второму входу (i+s)- го устройства хранения; (l-s+1)– й сервер подсоединен к первому входу (l-s+1)-го устройства хранения и ко второму входу первого устройства хранения, второй вход последнего l-го сервера группы подключен ко второму выходу s –го устройства хранения.

Приведем примеры формируемых вариантов конфигураций кластеров. Варианту конфигурации S1 (l=1, s=1) соответствует базовая конфигурация кластера, приведенная на рисунке 1. Варианту S2 (l=2, s=1) при m=4 соответствует конфигурация на рисунке 2 а), а варианту S3 (l=2, s=2) при m=4 – конфигурация на рисунке 1 б). Варианту S4 (l=m, s=1) соответствует конфигурация на рисунке 1 в), а варианту S5 (l=m, s=2) конфигурация на рисунке 1 г).

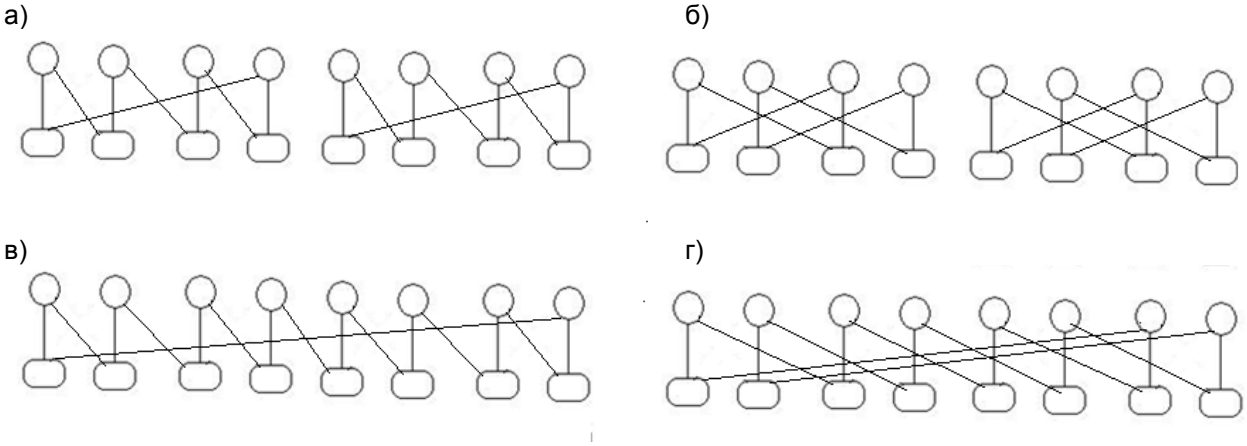


Рис. 2. Варианты конфигураций кластеров

Для рассматриваемых конфигураций число устройств хранения, подключаемых к каждому серверу два (*a=2*), число серверов, подключаемых к каждому устройству хранения два, максимальное число *b* устройств хранения, подключаемых к паре серверов приложений одного типа – четыре (для конфигураций S_5 и S_3), *b=ar=4*, а их минимальное число - два (для конфигураций S_1).

Максимальное число устройств хранения, суммарно подключенных к серверам приложений двух типов, равно восьми (для S_5), а минимальное равно четырем (для S_3 и S_1).

3. Сравнение вариантов конфигураций по детерминированным показателям отказоустойчивости. Сравнение отказоустойчивости конфигураций проведем детерминированным показателям: максимальное число отказов L, гарантированно выдерживаемых системой, и максимальное число отказов серверов приложений M , которое может выдержать система.

Сравнение проведем для определенного класса задач, для выполнения которых требуется исправность хотя бы одного сервера, выделенного под соответствующее приложение, при доступности для него хотя бы одного устройства хранения, без учета накопленных в нем данных предыдущих вычислений.

Для базовой конфигурации S1 потеря функциональности (доступности) серверов приложений, какого либо типа при кратности их резервирования r=2 возможна, если отказывает пара дублированных серверов этого типа или пара подключенных к ним устройств хранения.

Таким образом, для базовой конфигурации S1 минимальное число отказов, которое может привести к отказу системы B=2 и соответственно максимальное число отказов гарантированно выдерживаемых системой L=1. Для конфигураций по рис.2 а) и в) потеря доступности, какого либо типа серверов приложений возможна, если отказывает пара дублированных серверов одного типа или три из четырех связанных с ними устройств хранения.

Таким образом, для конфигурации по рис.2 а) и в) минимальное число отказов серверов, которое может привести к отказу системы B=2, а минимальное число отказов устройств хранения, которое может привести к отказу системы B=3. Максимальное число отказов гарантированно выдерживаемых системой по рис.2 а) и в) для серверов L=1, а для устройств хранения L=2. Конфигурации по рис.2 б) и г) гарантированно выдерживают максимальное число отказов для серверов L=1, а для устройств хранения L=3.

Таким образом, по показателю минимальное число отказов, которое гарантированно выдерживает система, доминирует конфигурации по рис. 2б) и г), а наихудшей является базовая конфигурация по рис .1.

Максимальное число отказов серверов приложений M, которое может выдержать система, для всех рассматриваемых конфигураций совпадает и равно m (если работоспособность сохраняют по одному серверу каждого типа).

Для конфигураций по рис.2 для серверов приложений двух типов работоспособность может поддерживаться одним устройством хранения, поэтому максимальное число отказов устройств хранения M, которое могут выдержать эти конфигурации равно 3m/2.

Максимальное число отказов устройств хранения M, которое может выдержать конфигурация S1 (рис 1) равно m, что подтверждает преимущество конфигураций по рис. 2 относительно конфигурации по рис.1.

Таким образом, показана большая отказоустойчивость конфигураций с максимальным числом устройств хранения, подключаемых к паре серверов приложений одного типа (b=B=4 для конфигураций S5 и S3).

5. Надежность конфигураций. Для конфигураций S1 при требовании исправности хотя бы одного сервера и одного устройства хранения в каждой из m дублированных групп вероятность безотказной работы вычислим как:[9]:

$$P_1(t) = \left\{ \left[1 - \left(1 - p_1(t)\right)^2 \right] \left[1 - \left(1 - p_2(t)\right)^2 \right] \right\}^m ,$$

где $p_1(t) = \exp(-\lambda_1 t), p_1(t) = \exp(-\lambda_1 t)$, λ_1, λ_2 интенсивность отказов сервера и устройства хранения.

Для конфигурации S_3 (рис. 1 в), вероятность безотказной работы группы определим как:

$$P(t) = \sum_{i=2}^{4} P_i(t),$$

где $P_i(t)$ вероятность работоспособных состояний с исправностью i из четырех серверов в группе (i=2,3,4),

$$P_4(t) = p_1(t)^4 \left[1 - \left(1 - p_2(t)\right)^4 \right].$$

$$P_3(t) = 4 p_1(t)^3 (1 - p_1(t))[p_2(t)^4 + 4 p_2(t)^3 (1 - p_2(t)) + 5 p_2(t)^2 (1 - p_2(t))^2 + 2 p_2(t)(1 - p_2(t))^3].$$

$$P_2(t) = 2 p_1(t)^2 (1 - p_1(t))^2 \left[1 - \left(1 - p_2(t)\right)^2 \right] + 2 p_1(t)^2 (1 - p_1(t))^2 \left[1 - \left(1 - p_2(t)\right)^2 \right]^2 =$$

$$= 2 p_1(t)^2 (1 - p_1(t))^2 \left[1 - \left(1 - p_2(t)\right)^2 \right] (1 + \left[1 - \left(1 - p_2(t)\right)^2 \right]).$$

Заключение. Проанализирована отказоустойчивость и надежность конфигураций кластеров с прямым подключением устройств хранения к дублированным серверам приложений m типов, в которых каждый сервер имеет два порта (входа) для подключения устройств хранения, а каждое устройство хранения два входа для подключения серверов. Для рассматриваемых систем показано преимущество по отказоустойчивости конфигураций с максимальным числом устройств хранения, подключаемых к каждой паре дублированных серверов, при минимизации числа устройств хранения, суммарно подключенных к серверам приложений двух типов.

Полученные результаты могут быть использованы при обосновании выбора конфигураций кластеров с прямым подключением устройств хранения к дублированным серверам.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность, №1, 2014. С. 69-77.
2. Джад Дж Основы проектирования SAN Brocade Bookshelf. San Jose, 2008 .589 с.
3. Clark T. The New Data Center . New technologies are radically reshaping the data center. Brocade Bookshelf. San Jose,2010 .156 p
4. Shooman M. Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design John Wiley & Sons, Inc 2002. 527 c
5. Воробьёв А.И., Татарникова Т.М. Применение генетического алгоритма для решения задачи обеспечения отказоустойчивости вычислительного кластера//Информационные технологии и системы: управление, экономика, транспорт, право, №1, 2011. С. 3-9.
6. Bogatyrev V.A. Fault tolerance of clusters configurations with direct connection of storage devices // Automatic Control and Computer Sciences 20011 45 (6) PP. 330 - 337
7. Bogatyrev V.A. Exchange of Duplicated Computing Complexes in Fault tolerant Systems // Automatic Control and Computer Sciences. – 2011. – V. 46. – № 5. – P. 268–276.
8. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оценка надежности отказоустойчивых кластеров с непосредственным подключением устройств хранения //Известия высших учебных заведений. Приборостроение. 2013. Т. 56. № 8. С. 77-81.
9. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения //Информационные технологии. 2013. № 2. С. 27-32.

УДК 681.3

ОРГАНИЗАЦИЯ МЕЖМАШИННОГО ОБМЕНА В КОМПЬЮТЕРНЫХ СИСТЕМАХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Богатырев Владимир Анатольевич[1], Богатырев Анатолий Владимирович[2],
Богатырев Станислав Владимирович[3],
[1]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
[2,3]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, д. 49,
e-mail: vladimir.bogatyrev@gmail.com.

Аннотация: исследуется эффективность вариантов объединения вычислительных комплексов в отказоустойчивую систему с организацией дублированных вычислений. Рассматриваются варианты межкомплексного обмена, в том числе, сочетающие внутрикомплексную и межкомплексную передачу через магистрали при различных дисциплинах доступа. Анализируется влияние организации обмена на надежность и отказоустойчивость системы.

Ключевые слова: *отказоустойчивость; вычислительная система; надежность; резервирование; дублирование; межкомплексный обмен; дисциплина доступа к магистрали.*

ORGANIZATION OF SAFE INTERCOMPUTER EXCHANGE IN COMPUTER SYSTEMS

Bogatyrev Vladimir [1], Bogatyrev Anatoly [2], Bogatyrev Stanislav [3],
[1]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21,
[2,3]St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverkskiy av. 49,
e-mail: vladimir.bogatyrev@gmail.com.

Abstract: Investigates the efficiency of computational complexes variants in a fault-tolerant system with the organization redundant calculations. Variants of an exchange between complexes through the bus at various disciplines access. Analyzes the impact of exchange on the reliability and resiliency of the system.

Keywords: *fault tolerance; computer system; reliability; redundancy; duplication; currency between computational complexes; discipline access to the bus.*

Введение. К компьютерным системам управления в реальном времени, в том числе к системам, связанным с безопасностью, предъявляются высокие требования по надежности и отказоустойчивости [1-6].

Системы, связанные с безопасностью, могут быть предназначены для предотвращения опасных событий или для смягчения (уменьшения риска) их последствий [3].

Обеспечение высокой надежности управляющих компьютерных систем, и особенно систем, связанных с безопасность, требует резервирования [1-5], как на уровне вычислительных узлов, так и на уровне их объединения в систему.

Таким образом, в отказоустойчивых компьютерных системах ответственного назначения, в качестве вычислительных узлов рекомендуется [1-5] использовать троированные или дублированные вычислительные комплексы (ДВК). При объединении ДВК в отказоустойчивую систему проводится резервирование ДВК и телекоммуникационных средств, в том числе магистралей (коммутаторов).

В компьютерных системах, работающих в реальном времени, и особенно, связанных с безопасностью, для повышения надежности вычислительного процесса в каждом полукомплексе ДВК вычисления дублируются, при этом контроль может включать сравнения результатов вычислений в полукомплексах, что снижает вероятность выдачи неправильных результатов.

1. Структура отказоустойчивой системы. Эффективность объединения ДВК при резервировании магистралей во многом определяется организацией межмашинного обмена. Рассмотрим в качестве базового вариант объединения ДВК в отказоустойчивую систему с дублированием магистралей по рис. 1.

Каждый из полукомплексов ДВК содержит процессор (P), модуль памяти (M), сетевые адаптеры (CA), адаптеры внутрикомплексной связи (A) и модуль контроля (S). Выполнение ответственных запросов дублируется в полукомплексах ДВК, контроль основан на сравнении результатов модулем S.

При дублированных вычислениях в результате межкомплексного обмена передаваемые данные должны быть занесены в модули памяти M двух полукомплексов адресуемого ДВК.

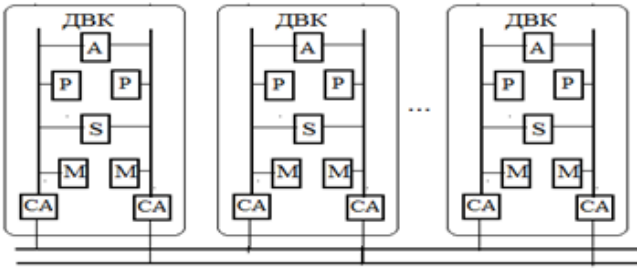


Рис.1 Объединение дублированных комплексов в систему

В работе исследуется эффективность вариантов объединения ДВК в отказоустойчивую систему с организацией дублированных вычислений. Для решения этой задачи рассматриваются варианты межкомплексного обмена, в том числе, сочетающие внутрикомплексную и межкомплексную передачу через магистрали при различных дисциплинах доступа и анализируется влияние организации обмена на надежность и отказоустойчивость системы.

При объединении ДВК в отказоустойчивую систему выделяется m основных и M-m резервных ДВК. Резервные ДВК выполняют вспомогательные вычисления, потеря которых не связана с безопасностью и значительными экономическими или иными потерями.

Для критичных вычислений выполнение каждого запроса дублируется в двух полукомплексах ДВК, результаты вычислений сравниваются модулем S и в случае их совпадения выдаются для дальнейшей обработки. При межкомплексном обмене для дублированных вычислений передаваемые данные должны быть занесены в модули памяти M двух полукомплексов адресуемого ДВК. При неспособности ДВК к дублированным вычислениям, например из-за отказов одного из процессоров, для обслуживания критичных запросов подключается один из резервных ДВК. Предусматривается восстановление ДВК после отказов, причем во время восстановления одного из полукомплексов, другой может выполнять некритичные вычисления (не требующих дублирование вычислительного процесса). При объединении ДВК в системы для внутрикомплексных обменов вместо адаптера A возможно использование пары CA.

2. Варианты организации межкомплексных обменов. Рассмотрим варианты организации обмена между ДВК при дублировании вычислений, когда необходимо занесение передаваемых данных в модули памяти M двух полукомплексов адресуемого ДВК [7],[8].

Для систем с дублированием магистралей и связью внутри ДВК выделим следующие варианты передачи от i-го к j-му ДВК:

Вариант B1: Первый и второй полукомплексы i-го ДВК выставляют запросы на доступ соответственно к первой M1 и ко второй магистралям M2 , после предоставления которых осуществляется передача CA1i→M1 →CA1j, CA2i→M2 →CA2j , в результате чего данные i-го ДВК поступают в модули памяти M обоих полукомплексов j-го ДВК.

Вариант B2: Множественный доступ реализуется только к одной магистрали, а вторая предоставляется вместе с первой, после чего осуществляется передача CA1i→M1 →CA1j, CA2i→M2 →CA2j .

Вариант B3: Первый либо второй полукомплексы i-го ДВК выставляют запросы на доступ соответственно к первой или ко второй магистралям M1 и M2 (закрепление за полукомплексами магистралей проводится так, чтобы обеспечить их равномерную загрузку). После предоставления магистрали Mg (g=1,2) i-му ДВК осуществляется передача CAgi→Mg →CAgj . В результате такой связи данные заносятся в модуль памяти M g-го полукомплекса j-го ДВК. Из модуля памяти g-го полукомплекса данные передаются в модуль памяти другого полукомплекса через адаптер внутренней связи A. Внутрикомплексная передача через адаптер A может быть параллельной.

Возможна модификация варианта B3, при которой запрос от ДВК выставляется одновременно к разным магистралям, но после предоставления доступа к одной из них, запрос на доступ к другой магистрали снимается на аппаратном уровне взаимодействия пары CA, что требует модификацию CA.

3. Надежность системы с учетом организации обмена. Сравним надежность системы ДВК с дублированнием магистралей межкомплексногообмена.

При дублировании вычислительного процесса взаимосвязь в системе каждого ДВК поддерживается:

– для вариантов обмена B1 и B2 при исправности двух его CA;

– для варианта обмена B3 либо при исправности адаптера внутрикластерной связи A и хотя бы одного из двух CA, либо при отказе адаптера внутрикластерной связи в случае исправности двух CA ДВК.

Коэффициент готовности кластера ДВК определим как:

$$P = \sum_{i=m}^{M} C_M^i r^i (1-r)^{M-i},$$

где r - коэффициент готовности ДВК с учетом работоспособности средств обмена, обеспечивающих дублированные вычисления.

Для кластера с вариантом обмена В1 (В2) коэффициент готовности ДВК r равен

$$r_1 = p p_{ca}^2 ,$$

а для варианта обмена В3 при внутрикомплексном обмене через адаптер А или через пару СА равны соответственно:

$$r_2 = p[p_a(1-(1-p_{ca})^2)+(1-p_a)p_{ca}^2],$$

$$r_3 = p[p_{ca}^2(1-(1-p_{ca})^2)+(1-p_{ca}^2)p_{ca}^2],$$

где *p* -коэффициент готовности базовой части ДВК (без учета средств обмена).

При реализации дублированного вычислительного процесса на двух полукомплексах с контролем:

$$p = \left(p_p p_m p_s\right)^2 .$$

Коэффициенты готовности узлов ДВК определяются как:

$$p_{ca} = \mu_{ca} / (\mu_{ca} + \lambda_{ca}), \;\; p_{ca} = \mu_{ca} / (\mu_{ca} + \lambda_{ca}), \;\; p_p = \mu_p / (\mu_p + \lambda_p) ,$$

$$p_m = \mu_m / (\mu_m + \lambda_m), \;\; p_s = \mu_s / (\mu_s + \lambda_s),$$

причем λ_p, λ_m , λ_s , λ_a,, λ_{ca} , – интенсивности отказов процессора, модуля памяти, схемы контроля, адаптера внутрикомплексной связи и СА , а μ_p, μ_m , μ_s , μ_a,, μ_{ca} интенсивности восстановлений соответствующих узлов.

Расчеты проведем при λ_a=λ_{ca}=0,00011/ч, μ_a= μ_{ca}=0,5 1/ч., и коэффициенте готовности базового оборудования ДВК *p* =0,9978. Полученные зависимости коэффициента готовности от числа ДВК представлены на рис. 2 а) при *M*=*m* и на рис 2 б) при *M*=*m*+1. На рис 2 а, b) кривая 1 соответствует коэффициенту готовности системы при варианте обмена В1(В2), а кривая 2 - при варианте обмена В3. Кривая 3 представляет разность *D* коэффициентов готовности структур при варианте обмена В3 при использовании для внутрикомплексного обмена адаптера А или пары СА. Проведенные расчеты показывают, что вариант обмена В3 при дублированных вычисления позволяет существенно повысить надежность кластера ДВК без увеличения расходов на его реализацию.

а) б)

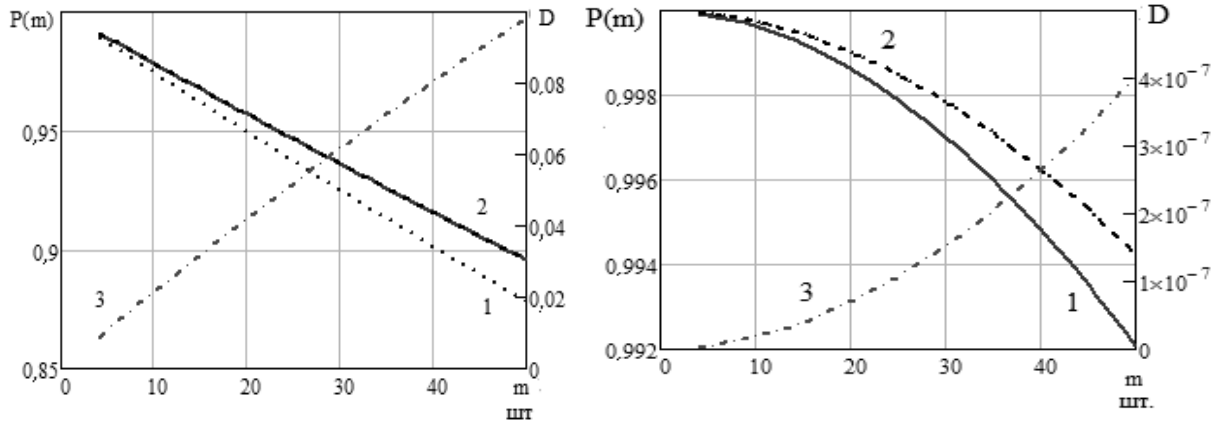


Рис .2. Коэффициент готовности а) при *M*=*m* , б) при *M*=*m*+1

Расчеты подтверждают эффективность ипользования в отказоустойчивых системах, объединяемых дублированные выислительные копмлексы межкомплексного обмена по варианту В3.

Заключение. Таким образом, при объединении ДВК в кластерные системы с организацией дублированных вычислений наиболее эффективен межкомплексный обмен В3 при передаче данных адресуемому ДВК по одной из магистралей с дальнейшей их внутрикомплексной передачей между модулями памяти полукомплексов адресуемого ДВК.

СПИСОК ЛИТЕРАТУРЫ

1. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб. Политехника . 2000.
2. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность, №1, 2014. С. 69-77.
3. Tatarnikova T., Kolbanev M. Statement of a task corporate information networks interface centers structural synthesis//IEEE EUROCON 2009, St. Petersburg, 2009. С. 1883-1887.

4. ГОСТ Р МЭК 61508-2:2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, связанным с безопасностью.
5. ГОСТ Р МЭК 61508-4:2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения.
6. ГОСТ Р МЭК 61508-6:2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2-2007 и ГОСТ Р МЭК 61508-3-2007.
7. Bogatyrev V.A. Fault tolerance of clusters configurations with direct connection of storage devices // Automatic Control and Computer Sciences 20011 45 (6) PP. 330 - 337
8. Bogatyrev V.A. Exchange of Duplicated Computing Complexes in Fault tolerant Systems // Automatic Control and Computer Sciences. – 2011. – V. 46. – № 5. – P. 268–276.

УДК 004.056.5

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ВНУТРИКОРПОРАТИВНЫХ ПОЛИТИК БЕЗОПАСНОСТИ НА ПРИМЕРЕ МАЛОГО ПРЕДПРИЯТИЯ

Емельянов Александр Александрович,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mail: S1_Alex2000@mail.ru.

Аннотация: проводится исследование некоторых видов угроз информационной безопасности в рамках малого предприятия, и приводятся результаты разработки политик безопасности, направленных на их устранение.

Ключевые слова: *информационная безопасность; уязвимости; защита; Radius.*

PRACTICAL IMPLEMENTATION OF SECURITY POLICY IN SMALL BUSINESS CASE

Emelyanov Alexandr,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: S1_Alex2000@mail.ru.

Abstract: article contains results of research for some type's threats to information security in small business and demonstrating elimination of them with security policies.

Keywords: *information security; vulnerabilities; defense; Radius.*

Введение. Перед автором была поставлена задача обеспечить информационную безопасность (ИБ) в рамках информационной системы (ИС) малого предприятия «СпецСервис». Данное малое предприятие оказывает посреднические услуги.

Структура предприятия. Существует семь основных офисов, связанных в единую сеть с использованием гетерогенной структуры (применяются как проводные, так и беспроводные каналы передачи данных).

Менеджеры компании используют для выполнения своих функциональных обязанностей персональные компьютеры с операционной системой Windows.

Коммерческой ценностью являются базы данных клиентов, поставщиков, актуальных расценок на различные группы товаров, контактных данных связанных с компанией физических и юридических лиц, личные данные работников.

В процессе работы необходимо, с одной стороны, обеспечить возможность работы сотрудников предприятия с вышеуказанными данными, с другой – предотвратить несанкционированный доступ, порчу и хищение информации.

Процедура построения модели угроз информационной безопасности состоит из нескольких последовательных шагов:

– Определение источников угроз.
– Выявление критических объектов информационной системы.
– Определение перечня угроз для каждого критического объекта.
– Выявление способов реализации угроз.
– Оценка материального ущерба и других последствий возможной реализации угроз.

Политика информационной безопасности предприятия – это совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и разграничение доступа к информационным ресурсам.

В соответствии с документом, регламентирующем политику безопасности на предприятии, необходимо было выработать оптимальный комплекс мер, направленных на уменьшение вероятности проявления событий, могущих нанести вред деятельности учреждения. В связи с этим требовалось определить угрозы: как внутренние, так и внешние; как псевдослучайные, так и

преднамеренные. Важно установить также весовые коэффициенты (степень опасности) угроз. Это необходимо для того, чтобы, с одной стороны, устранить опасность того или иного фактора, с другой – минимизировать ограничения в работе предприятия.

По сути, разработка политик безопасности и их реализация является поиском оптимального баланса между двумя крайними ситуациями: полностью закрытой и нефункциональной системой, обеспечивающей максимальную степень безопасности; и целиком открытой, удобной и быстродействующей, но при этом не защищенной от любого вида внешних и внутренних угроз.

В ходе работы были выявлены основные уязвимые места в соответствии с [1]. Проведенный анализ воздействий на информацию и несанкционированного доступа к ней показал, что их можно разделить на псевдослучайные и преднамеренные [1, 2].

Псевдослучайный характер угроз подразумевает воздействие на информационные потоки/носители данных/вычислительные системы, имеющее результат в виде повреждения информации либо несанкционированного доступа.

Примеры: недоступность веб-сервера из-за отключения электроснабжения (предсказание отказов электросети невозможно, но обеспечение дополнительного источника питания (UPS, ИБП) вполне реализуемо); повреждение данных файлового сервера (случайный выход из строя поверхности диска и отсутствие при этом системы резервного копирования на базе RAID-массива).

Преднамеренный характер угроз связан с заранее спланированными действиями человека/группы людей, направленными на неправомочный доступ/искажение информации, критически важной для корректного функционирования предприятия. Причинами могут быть недовольство жизненной ситуацией, сугубо материальный интерес или развлечение с самоутверждением способностей.

Для создания средств защиты информации необходимо было определить сферы вредоносного воздействия, формы и пути их возможного проявления и осуществления в рассматриваемой автоматизированной системе. Для решения поставленной задачи все многообразие угроз и путей их воздействия было приведено к простейшим видам и формам, которые адекватны их множеству в реальной среде.

В документе, регламентирующем политику безопасности предприятия, определены следующие требования к информационной безопасности:

1. Блокировка возможности хищения информации с помощью подключения внешних флеш-носителей, оптических дисков, жёстких дисков, сетевых устройств
2. Запрет передачи данных через коммуникационные порты ПК
3. Запрет несанкционированного подключения личных устройств (ноутбуки, КПК, планшеты, смартфоны)
4. Недопущение входа во внутреннюю логическую сетевую инфраструктуру при скрытом физическом внедрении незарегистрированного устройства в аппаратную часть ЛВС.

Для реализации указанных требований сформулированы и предложены рекомендации для системных администраторов предприятия:

– на всех рабочих станциях снять CD/DVD-приводы;
– заблокировать на уровне BIOS порты USB, COM, LPT;
– на вход в конфигурационную систему CMOS установить пароли;
– для исключения возможности скачивания информации из сети при помощи несанкционированно подключаемых сетевых устройств (ноутбуки, нетбуки, NAS, КПК и т.д.) ввести потоковое шифрование трафика на каждой рабочей станции и сервере при помощи протокола IPSec [2,4].

Генерация сертификатов, с помощью которых происходит согласование криптографических алгоритмов при установлении соединения, осуществляется центром сертификации (ЦС) на базе ОС Linux (ветвь CentOS). После создания сертификатов они были импортированы на рабочие станции и серверы.

В соответствии с требованиями заказчика в рамках одной из подсетей следовало исключить не только возможность скачивания информации при подключении несанкционированного сетевого устройства, но и сделать невозможным подобное подключение. Для этого использовался механизм аутентификации по протоколу 802.1X. В качестве Radius – сервера использовалась система Linux (линейка Fedora). Применялся пакет FreeRadius. Аутентификация производится при помощи бинарного ключа: MAC-адреса и сертификата.

В роли базовой модели коммутатора, который выполняет роль аутентификатора, был выбран управляемый вариант D-Link DES-3828. входящий в семейство D-Link xStack. Он обеспечивает высокую производительность (24 порта 100BASE-TX и 4 порта 1000BASE-T), реализует стандарт 802.1X, управление на основе MAC-адресов (до 16 на порт), обеспечивает аутентификацию через сервер RADIUS, дополнительно имеет ACL, обеспечивает регистрацию событий по протоколу syslog на сервер и, помимо прочего, поддерживает управление по SSH.

Для устранения угроз псевдослучайного характера в рамках каждого пакета серверов был установлен независимый источник бесперебойного питания и дисковый RAID-массив уровня 1

(зеркалирование). Реализовано автоматическое ежесуточное создание резервных копий системы всех серверов на сетевом накопителе NAS. Данная мера показала свою эффективность в первые два месяца после завершения внедрения.

Линии связи с внешней сетью были выполнены в виде трех независимых каналов передачи данных: оптико-волоконная линия, проводной канал «витая пара» и беспроводной модем.

Автоматическая балансировка нагрузки и динамическое перераспределение сетевого трафика в случае выхода из строя какого-либо из каналов передачи данных позволяет свести к минимуму вероятность полной информационной изоляции предприятия из-за отказа связи [4,5]

Выводы: в рамках любого предприятия, вне зависимости от его размерности, рода деятельности, территориальной обособленности и прочих характеристик необходима тщательная проработка информационной инфраструктуры, важнейшим компонентом которой является системы локальной и сетевой безопасности.

В случае, если данному аспекту уделяется недостаточное количество ресурсов, с высокой степенью уверенности можно сказать, что затраты на устранение последствий псевдослучайных и преднамеренных воздействий, приводящих к ограничению функционирования либо полной остановке деятельности предприятия, будут весьма велики. Разработка и внедрение системы информационной безопасности в рамках малого предприятия «СпецСервис» позволило свести к минимуму угрозы несанкционированного доступа, хищения и повреждения коммерчески важной информации и подтвердило эффективность созданной системы защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э. Современные операционные системы. СПб.: Питер, 2010.
2. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. СПб.: Питер, 2009
3. Пуха Г.П. Методология формирования и реализации систем интеллектуальной поддержки принятия решений. СПб.: СМИО-Пресс, 2012.
4. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения //Информационные технологии. 2013. № 2. С. 27-32.
5. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оценка надежности отказоустойчивых кластеров с непосредственным подключением устройств хранения //Известия высших учебных заведений. Приборостроение. 2013. Т. 56. № 8. С. 77-81.

УДК 004.056.53

СИСТЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ КАК СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Золотарева Екатерина Николаевна,
Россия, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
ул. Кронверская, д. 49,
e-mail: katerina2794@rambler.ru

Аннотация. В статье описываются проблемы обеспечения информационной безопасности в области конфиденциальных данных без применения специализированных средств, рассматриваются возможные пути решения данной проблемы.

Ключевые слова. *Привилегированные пользователи, привилегированные учетные записи, DLP – системы.*

CONTROL SYSTEM PRIVILEGED USERS AS A MODERN MEANS OF INFORMATION PROTECTION

E.N. Zolotareva,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: katerina2794@rambler.ru

Abstract: This article describes the information security problems in the area of sensitive data without the use of specialized tools, possible ways of solving this problem.

Keywords*: Privileged user, privileged accounts, DLP – system.*

Введение. Создание систем информационной безопасности (СИБ) в ИС и основывается на комплексном подходе, который заключается в следующих принципах, перечисленных ниже.

– Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

– Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ.

Способы реализации угроз информации в ИТ непрерывно совершенствуются, а потому обеспечение безопасности ИС не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа.

– Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т.е. предоставление как пользователям, так и самим работникам ИС, минимума строго определенных полномочий, достаточных для выполнения ими своих служебных обязанностей.

– Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИТ без ее предварительной регистрации.

– Обеспечение надежности системы защиты, т.е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

– Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

– Обеспечение всевозможных средств борьбы с вредоносными программами.

– Обеспечение экономической целесообразности использования системы. защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации.

Система информационной безопасности, как и любая ИС, должна иметь определенные виды собственного программного обеспечения, опираясь на которые она будет способна выполнить свою целевую задачу, организовать политику безопасности.

Реализация политики безопасности требует настройки средств, управления системой защиты и осуществления контроля ИС (организационные методы). Как правило, задачи управления и контроля решаются административной группой, состав и размер которой зависят от конкретных условий. Очень часто в эту группу входят администратор безопасности, менеджер безопасности и операторы.

Особой популярностью и большим спросом пользуются DLP-системы – решения по контролю выхода конфиденциальной информации за периметр компании.

Технологии DLP – это компоненты или модули анализа информации, которая передается по самым распространенным каналам передачи данных, таким как съемные носители, печать, корпоративная почта, любые вариации, связанные с веб-направлением (с отправкой данных через протокол HTTP), но на практике с помощью DLP-системы нельзя контролировать всю конфиденциальную информацию, поэтому существуют отдельные классы продуктов, которые позволяют защитить компанию от рисков утечки конфиденциальных данных. Самым существенным риском для каждой организации являются привилегированные пользователи, обладающие расширенными правами доступа на компьютере, серверах или в других системах, тем самым повышая уровень угрозы утечки информации [5].

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.

Данные системы контроля позволяют анализировать то, что происходит на файловом ресурсе, отслеживать модель поведения пользователя. Если по каким-то параметрам она противоречит его обычному поведению, система выдает оповещение.

Данная система упрощает доступ к сетевым информационным ресурсам для сотрудников организации, при этом повышается уровень защиты корпоративных информационных систем. Централизованная система, управления привилегированных учетных записей привилегированных пользователей, позволяет отслеживать все привилегированные учетные записи и обычные учетные записи в подключенных информационных системах. Помимо управления привилегированными учетными записями пользователей, система контроля привилегированных пользователей

обеспечивает аудит прав в информационных ресурсах, сигнализируя о несанкционированных изменениях полномочий [4].

Данная система предоставляет отчетность обо всех учетных записях и правах доступа привилегированных пользователей организации в интегрированных с системой контроля привилегированных пользователей информационных системах.

Основные задачи системы контроля привилегированных пользователей следующие:

– автоматизация процесса управления идентификационными данными;
– единообразие (унификация) учетных данных пользователей;
– централизованное управление правами доступа;
– сокращение расходов на администрирование информационных систем и обслуживание пользователей;
– снижение рисков несанкционированного доступа к корпоративным информационным системам;
– сокращение временных затрат на предоставление, изменение и отзыв прав доступа привилегированных пользователей;
– соответствие требованиям законодательных актов: 152-ФЗ «О персональных данных», руководящих документов ФСТЭК и ФСБ: Приказ ФСТЭК от 18 февраля 2013 г. № 21, отраслевых стандартов: частности СТО БР ИББС-1.0-2014 и PCI DSS.

На сегодняшний день среди систем контроля привилегированных пользователей востребованы аналитические или дополнительные системы, контролирующие права доступа к целевым бизнес-ресурсам.[2], [3].

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 (Corporate Performance Management, CPM).

Цель аналитической системы – преобразовать большое количество данных, останавливаясь на ключевых факторах эффективности, моделируя исход различных вариантов действий, отслеживая результаты принятия решений.

Аналитические системы поддерживает множество бизнес-решений – от операционных до стратегических. Основные операционные решения включают в себя позиционирование продукта или цен [1]. Стратегические бизнес-решения включают в себя приоритеты, цели и направления в самом широком смысле. Система наиболее эффективна, когда она объединяет данные, полученные из рынка, на котором работает организация (внешние данные), с данными из источников внутри организации, таких как финансовые и операции данные (внутренние данные).

В сочетании, внешние и внутренние данные дают полную картину бизнеса, которая, создает «интеллект» – быстрое понимание, которое не получить из простого набора данных.

СПИСОК ЛИТЕРАТУРЫ

1. М. Башлыков [Электронный ресурс]: «Управление привилегированным доступом имеет особое значение для бизнеса» -// М. Башлыков электронные данные.
2. Стандарт ISO 27001, PCI DSS
3. Асаул А.Н. [Электронный ресурс]: « Организация предпринимательской деятельности: Информационная безопасность» –// А.Н. Асаул электронные данные.
4. Глухов Н.И., Краснощек А.А.: Методические вопросы оценки информационных рисков предприятий железнодорожного транспорта/ Глухов Н.И., Краснощек А.А.//Экономика, экономические науки.
5. http://www.securitylab.ru/blog/company/Softline/35233.php [Электронный ресурс]

УДК 004.056

АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТРИК

Канев Антон Николаевич,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
e-mail: kanev.a.n@mail.ru

Аннотация: В статье рассмотрен процесс анализа уязвимостей информационной системы, а также разработанная методика, предлагающая комплексное решение по анализу уязвимостей на основе метрик. Данная методика предполагает использование баз данных уязвимостей и сканеров уязвимостей для выявления уязвимостей. Затем предлагается провести классификацию уязвимостей с выделением категорий и классов уязвимостей. Последние характеризуются заданным набором метрик, значения которых определяются инструментальными средствами или экспертами. С

помощью метода парных сравнений производится расчет приоритетов метрик классов уязвимостей, необходимых для определения степени опасности класса уязвимостей и впоследствии категорий уязвимостей. Преимуществом методики является охват широкого спектра уязвимостей информационной системы с использованием единого подхода к их оценке.

Ключевые слова: *анализ уязвимостей, информационная система, метрика.*

INFORMATION SYSTEM VULNERABLITY ANALYSIS BASED ON METRICS

Kanev Anton,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: kanev.a.n@mail.ru

Abstract: The article presents the process of the information system vulnerability analysis and the developed methods, which offer a comprehensive solution of vulnerability analysis based on metrics. The given methods supposes using vulnerability databases and vulnerability scanners for vulnerability detection. Then it is offered to conduct a classification into categories and classes. Classes are characterized by the given set of metrics the value of which is defined by tools or experts. The method of pairwise comparison is offered for metric priority computation of vulnerability classes which is required for a definition of vulnerability class danger and vulnerability category danger afterwards. The advantage of methods is wide range coverage of information system vulnerabilities with the single vulnerability assessment approach.

Keywords: *vulnerability analysis, information system, metric.*

Введение. Анализ уязвимостей информационной системы (ИС) – сложный процесс. Перед аналитиком встают задачи обнаружения уже известных уязвимостей, поиска новых уязвимостей, а также последующая оценка опасности выявленных уязвимостей [1]. На сегодняшний день отсутствует комплексная методика анализа уязвимостей. Чаще всего проводится анализ уязвимостей программного обеспечения (ПО), при этом не рассматриваются уязвимости технических средств (ТС), организационные и прочие уязвимости.

Цель работы – разработка комплексной методики анализа уязвимостей ИС. Для достижения поставленной цели выполнены следующие задачи:

- характеристика процесса анализа уязвимостей ИС;
- рассмотрение современных подходов к оценке уязвимостей ИС;
- формирование основных положений методики анализа уязвимостей;
- формирование модели оценки уязвимостей ИС;
- разработка модуля анализа уязвимостей ИС.

Разработанная методика анализа уязвимостей ИС предлагает комплексное решение по анализу уязвимостей, который включает процедуру выявления уязвимостей ИС и процедуру оценки уязвимостей ИС [1].

На этапе выявления уязвимостей предполагается выявление уязвимостей ПО с использованием базы данных известных уязвимостей Common Vulnerabilities and Exposures (CVE) и Common Configuration Enumeration (CCE), а также средств контроля защищенности, основанные на применении способов обнаружения уязвимостей.

Для оценки уязвимостей ИС была сформирована иерархическая модель оценки уязвимостей ИС, которая основана на классификации уязвимостей ИС. На первом уровне классификации располагаются категорий уязвимостей [2]. На втором уровне располагаются сходные уязвимости в категории, объединенные в классы. Классы характеризуются заданным набором метрик, значения которых определяются инструментальными средствами или экспертами.

Метрики принимают значения в диапазоне [0;1] и оценивают соответствующий им показатель. Показатели могут принимать различные значения. Значения метрик для качественных показателей рассчитываются с использованием метода парных сравнений. Оценка уязвимостей кода ПО и уязвимостей конфигурации ПО производится на основе систем оценок Common Vulnerability Scoring System (CVSS) и Common Configuration Scoring System (CCSS) соответственно.

С помощью метода парных сравнений производится расчет приоритетов метрик классов уязвимостей. Таким образом, степень опасности класса уязвимостей определяется следующим выражением [3]:

$$x_i = \sum_k \sum_j \lambda_{ij} w_{jk}, \quad (1)$$

где

x_i – степень опасности класса уязвимостей,

w_{jk} – выбранные значения метрик,

λ_{ij} – приоритеты метрик относительно классов уязвимостей.

Для расчета степени опасности категории уязвимостей применяется следующее выражение:

$$h = 1 - \sqrt[N]{\prod_{i=1}^{N}(1 - x_i)}, \qquad (2)$$

где h – степень опасности класса уязвимостей,

x_i – степень опасности класса уязвимостей,

N – количество классов уязвимостей в категории. При этом оценка рассчитывается для единственного компонента ИС из возможных в данной категории.

С целью получения интегральной оценки степени опасности категории уязвимостей используется следующее выражение:

$$H = \sum_{i}^{n} \frac{1}{2^i} h_i, \qquad (3)$$

где H – интегральная оценка степени опасности категории уязвимостей,

n – количество компонентов, уязвимости которых входят в данную категорию,

h_i – оценка степени опасности уязвимостей *i*-ого компонента, а компоненты сортированы по убыванию оценки.

На основе предложенной методики анализа уязвимостей ИС был разработан программный модуль на базе интеграционной платформы RSA Archer eGRC [4]. Модуль анализа уязвимостей осуществляет сбор, хранение и обработку исходных данных о компонентах ИС и их уязвимостях, расчет оценок степени опасности уязвимостей и представление результатов на информационных панелях, пример одной из которых приведен на рисунке 1.

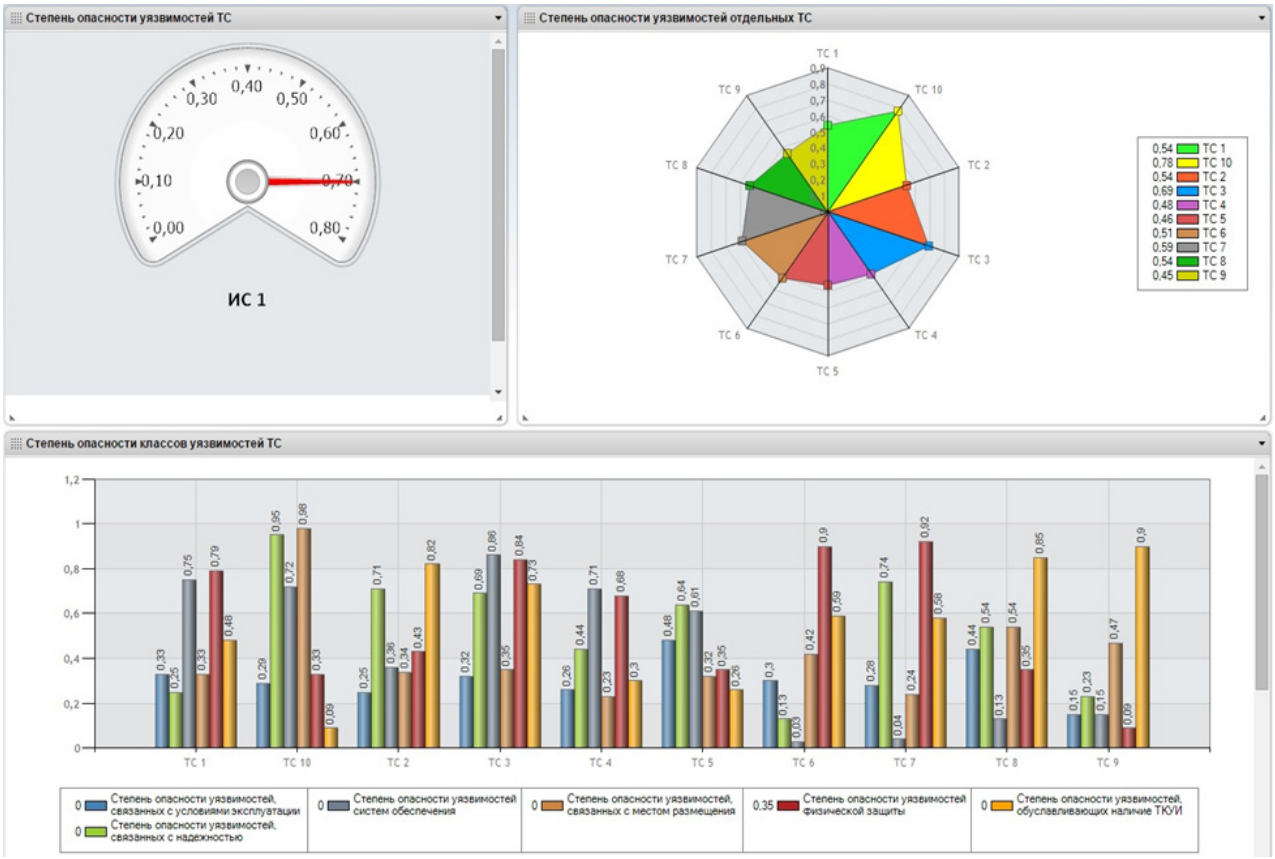


Рис. 1. Информационная панель «Оценка уязвимостей технических средств» модуля анализа уязвимостей ИС

Заключение. Преимуществами данной методики является охват широкого спектра уязвимостей ИС 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 ИС. Разработанная методика может представлять интерес для организаций, сталкивающихся с проблемой анализа уязвимостей ИС, а результаты ее применения используются для анализа рисков информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Проект ГОСТ Р XXXXX-20XX. Защита информации. Уязвимости информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем.
2. Проект ГОСТ Р XXXXX-20XX. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.
3. Подвесовский А.Г. Метод анализа иерархий (теория) // Брянский государственный технический университет. – 2013. – Электронный ресурс] – URL: http://www.studfiles.ru/preview/3874267 – Режим доступа: свободный; дата обращения: 18.09.2015.
4. Борисенко П.С., Ильин И.В., Канев А.Н., Никифорова К.А. Анализ современного рынка продуктов GRC // «Научное сообщество студентов XXI столетия. Технические науки»: Электронный сборник статей по материалам XXXI студенческой международной научно-практической конференции. – Новосибирск: Изд. «СибАК». – 2015. – № 4 (30) / [Электронный ресурс] – URL: http://www.sibac.info/archive/technic/4(30).pdf –Режим доступа: свободный; дата обращения: 18.09.2015.

УДК 004.9

ПРЕДМЕТНАЯ ОБЛАСТЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Касаткин Виктор Викторович[1], Колбанев Михаил Олегович[2], Татарникова Татьяна Михайловна[3],
[1] Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова,
Россия, Санкт-Петербург, 1-я Красноармейская ул., д. 1,
[2,3] Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mails: v.v.kasatkin@mail.ru, mokolbanev@mail.ru, tm-tatarn@yandex.ru

Аннотация: Предлагается обобщенная модель информационного взаимодействия, изучение которой позволяет комплексно подходить к решению многих практических задач и выбирать эффективные решения по организации информационного взаимодействия в интересах той или иной предметной деятельности, где реализуется данная модель.

Ключевые слова: *двухуровневую модель информационного взаимодействия людей; информационный процесс; схема технической системы связи К. Шеннона; обобщенная модель информационного процесса при помощи технических средств; предметная область.*

THE SUBJECT AREA OF INFORMATION INTERACTION

Kasatkin Victor [1], Kolbanev Mikhail [2], Tatarnikova Tatiana[3],
[1] The Baltic State Technical University, named after D.F. Ustinov,
Russia, St. Petersburg, 1-st Krasnoarmeyskaya str., 1,
[2,3] Saint-Petersburg State University of Economics,
Russia, St. Petersburg,Sadovaya str., 21,
e-mails: v.v.kasatkin@mail.ru, mokolbanev@mail.ru, tm-tatarn@yandex.ru.

Abstract: Offers a generalized model of information interaction, the study of which allows for complex approach to the solution of many practical problems and to choose effective solutions for organization of information interaction in the interests of one or another subject that implemented this model.

Keywords: t*wo-level model of information interaction of people; information process; the scheme of technical communication system by Claude Shannon; generalized model of information through technical means, subject area.*

Введение. Общие законы и закономерности информационного взаимодействия в природе и обществе реализуются через информационные процессы двух типов: процессами мышления людей и процессами выполнения операций над данными, как материальными объектами, которые представлены знаками языка взаимодействия[1]. Эти процессы образуют иерархию информационного взаимодействия, приведенную на рисунке 1. Таким образом, информационный процесс – это последовательность операций преобразования данных на материальном метауровне, которая поддерживает интеллектуальное взаимодействие людей на идеальном метауровне[2].

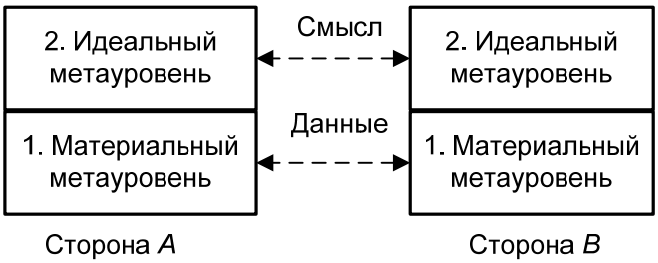


Рис. 1. Иерархическое представление информационного взаимодействия

Информационный процесс может быть:

– естественным, протекающим по объективным законам природы как данность человеку;

– искусственным, протекающим при помощи технических средств, созданных людьми для расширения возможностей информационного взаимодействия друг с другом.

1. Обобщенная модель информационного процесса. Одной из первых обобщенных моделей искусственного информационного процесса на материальном метауровне является общая схема системы связи К. Шеннона [3], которая предназначена для «точного или приближенного переноса сообщения между двумя точками пространства» (рисунок 2).

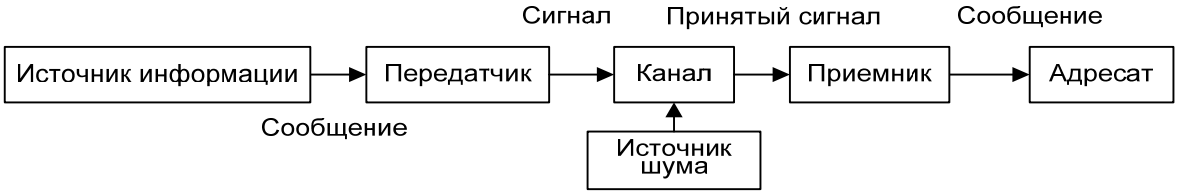


Рис. 2. Общая схема системы связи К.Шеннона

Схема устанавливает, что в процессе переноса от передающей на приемную сторону при помощи технических средств данные должны менять представление, получая форму сообщений и сигналов, но во всех случаях несут один и тот же смысл, сгенерированный источником информации. Источник информации создает сообщение или последовательность сообщений, которые должны быть переданы на приемный конец. Передатчик некоторым образом перерабатывает сообщения в сигналы, соответствующие характеристикам канала. В процессе передачи сигнал может быть искажен шумом. Канал – это среда, используемая для передачи сигнала от передатчика к приемнику. Приемник выполняет операцию, обратную по отношению к операции передатчика, восстанавливая сообщение по сигналам, и передает его адресату. Адресат – это получатель адресованной ему информации источника.

В схеме К. Шеннона не учитывается влияние смысла и физической формы представления данных на процесс взаимодействия. Если учесть, что взаимодействие реализуется физической средой, которая обеспечивает преобразование временной, пространственной и физической координат данных таким образом, чтобы они стали доступны получателю, то тогда объектами для преобразования являются:

1) время доступности данных для использования,

2) пространственное расположение данных,

3)физическая форма представления данных.

Способность среды взаимодействия изменять временную, пространственную координаты и физическую форму сигнала превращает ее, соответственно, в:

– память – это среда для записи (сохранения) сигналов в момент доступа источника и считывания (снятия) сигналов в момент доступа получателя;

– канал связи – это среда для передачи сигналов в пространстве от источника к получателю;

– обработчик данных – это среда для изменения физической формы сигнала между моментами доступа источника и получателя.

Среда взаимодействия сохраняет сигнал (свойство памяти), распространяет сигнал (свойство канала связи) и изменяет форму сигнала (свойство обработчика данных). Количественное проявление этих свойств зависит от вида сигнала и внешнего управления.

Если учесть влияние смысла, то введем обобщающее понятие коммуниканта.

Коммуниканты – это материальные объекты, которые обладают интеллектом, способны понимать контекст информационного взаимодействия, генерировать и осваивать информацию.

На материальном метауровне коммуниканты должны различать знаки языка взаимодействия, то есть устанавливать совпадение и различие между знаками из информационного базиса и определять порядок следования знаков друг за другом во времени и пространстве. Разделение коммуникантов на источник и адресат условно. Их роли могут меняться:

1. Обратная связь превращает информационный процесс в диалог.

2. Источник информации может быть, одновременно, и получателем, например, обработанной или сохраненной информации.

Кроме этого источник и получатель информации могут находится в разных точках как временной, так и пространственной осей существования материальных объектов.

Таким образом, если учесть все введенные выше добавления к схеме на рисунке 2, то информационный процесс в общем виде, реализуемый при помощи технических средств, включает (рисунок 3):

1) материальные объекты для преобразования информации и данных – это:

– коммуниканты, выполняющие роли источника и получателя информации,

– среда взаимодействия, обеспечивающая преобразование координат сигнала,

– сигнальные устройства, которые превращают при передаче сообщение в сигнал, а при приеме – сигнал в сообщение;

2) информационные объекты – это:

– информация коммуникантов;
– данные в форме сообщений и сигналов;

3) воздействия со стороны внешней среды – это:

– помехи;
– управления средой взаимодействия.

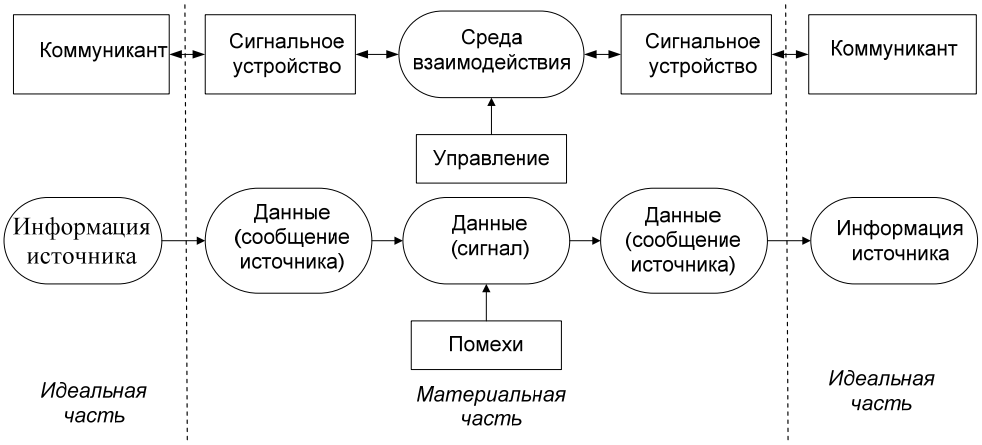


Рис. 3. Обобщенная модель информационного процесса

Обобщенная модель учитывает 3 типа взаимодействия:

– во времени,
– в пространстве и
– путем обработки данных.

К. Шеннон выделил 3 типа информационных объектов, используемых для организации информационного взаимодействия: сообщения, данные и сигналы.Все эти объекты несут один и тот же смысл, созданный источником.

Сообщение – это данные в виде кодовой последовательности знаков языка взаимодействия, созданные коммуникантом. Главное в сообщении – это то, что оно несет смысл, закодированный на языке, который понятен получателю, но сам смысл никак не влияет на свойства сообщения и остается за пределами схемы К. Шеннона.

Данные – это обобщенное обозначение для любой информации, представленной в материальной форме. Если абстрагироваться от смысла сообщения, то оно представляет собой данные информационного взаимодействия, и, наоборот, данные превращаются в сообщение только для такого коммуниканта, который понимает заложенный в них смысл.

Сигнал – это те же данные, но имеющие физическую форму, обеспечивающую их перемещение от источника к получателю при помощи физической среды взаимодействия – памяти, канала связи или обработчика. Сигнал – это носитель (переносчик) смысла в физическом пространстве.

Если объединить двухуровневую модель информационного взаимодействия людей (рисунок 1), схему технической системы связи К. Шеннона (рисунок 2) и сделанные обобщения функций коммуникантов, сигнальных устройств и физической среды (рисунок 3), тополучим обобщенную модель информационного взаимодействия людей при помощи технических средств [2] (рисунок 4).

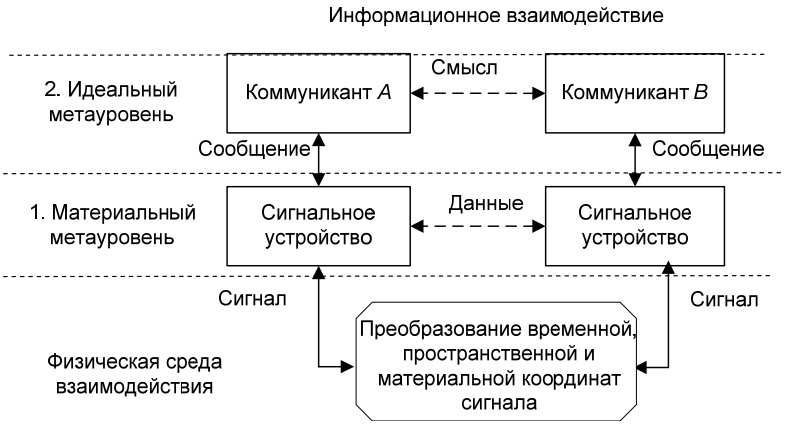


Рис. 4. Обобщенная модель информационного взаимодействия людей при помощи технических средств

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

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

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

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

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

1) эффективность создания и использования интеллектуального потенциала на идеальном метауровне зависит от организации информационных процессов преобразования данных на материальном метауровне.

2) эффективность информационных процессов материального метауровня зависит от используемой информационной технологии.

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

4) эффективность функционирования физической среды взаимодействия определяется объемом потребления физических ресурсов по отношению к реализованным информационным и интеллектуальным процессам [4].

Примеры применения обобщенной модели информационного взаимодействия людей при помощи технических средств. Рассмотрим несколько примеров применения модели.

Пример 1. Можно выделить 3 типа образовательных направлений в области информационных наук [5]:

– метауровень проблемной области – изучение методов применения информационных технологий для создания, проектирования и эксплуатации социальных, биологических и технических систем во всевозможных проблемных областях. Основные дисциплины: информационные системы в экономике, управлении, медицине, проектировании, строительстве и т.д. Здесь разрабатываются средства автоматизации процессов в проблемных областях. Пример образовательных направлений: бизнес-информатика, прикладная информатика.

– метауровень преобразования данных – методические и программно-аппаратные средства реализации информационных процессов сохранения, распространения и обработки данных. Основные дисциплины: архитектура систем, операционные системы, программирование, базы данных, схемотехника, цифровая техника, интеграция распределенных информационных ресурсов, интеллектуализация, безопасность информационных систем, теория связи и др. Пример образовательных направлений: информационные системы и технологии, инфокоммуникационные сети и системы связи.

– физическая среда – базовые технологии информатизации, основанные на законах физики: микро(нано)электроника, фотоника, радиотехника и др.

Пример 2. Можно выделить 3 группы методов обеспечения безопасности процессов информационного взаимодействия [6]:

– на идеальном метауровене обеспечивается защита смыслов с учетом человеческого фактора. Человек, обладающий секретным знанием, рассматривается как часть системы и одно из уязвимых мест в системе безопасности. Разрабатываются мероприятия, блокирующие такие ошибки людей, которые могут привести к успешным информационным атакам, имеющим цель раскрыть секретные смыслы противнику;

– на материальном метауровене обеспечивается защита логических свойств сообщений, составленных на том или ином языке информационного взаимодействия, например, математическими методами криптографии путем перевода смыслов на язык, который не знает противник. Шифрование, цифровая подпись и др.;

– на уровне физической среды обеспечивается защита сигнала и физических законов его существования, например, от попыток разрушить или модифицировать память, от перехвата побочных излучений или наводок медного кабеля, от воздействия на сигналы программным путем и др.

Пример 3. Можно выделить три метауровня информационного взаимодействия в сервисной деятельности. Отметим, что особенности сервиса заключаются в том, что он во-первых, имеет форму информационного взаимодействия между людьми – клиентом и оператором услуги и во-вторых,

предоставляет услугу в виде процесса, который не связан с получением клиентом права владения чем-либо, но приносит клиенту некоторую пользу в ходе своей реализации [4]. Тогда:

– идеальный метауровень сервиса отображает смысловое взаимодействие оператора с клиентами. Здесь формируются и изучаются описания услуг, разрабатываются коммерческие предложения, учитываются требования клиентов к качеству обслуживания и т.п.;

– материальный метауровень сервиса отображает процессы обмена данными, которые со сторон и клиента, и оператора поддерживаются мультимедийными терминалами (компьютер, смартфон, планшет и др.). Мультимедиа технологии позволяют в наиболее привлекательной форме представить клиенту описание и условия предоставления услуги;

– физическая среда взаимодействия может быть организована в вычислительном облаке, которое независимо от местоположения клиентов и оператора при помощи центров обработки данных, центров обслуживания вызовов или других программно-аппаратных инфокоммуникационных сред обеспечит физическое сохранение, распространение и обработку сигналов, поддерживая процесс предоставления услуги.

Пример 4. Можно выделить три метауровня информационного взаимодействия при изучении предметной области. Отметим, что предметная область – это совокупность элементов реального мира и связей между ними, которую предполагается изучать с целью организации и автоматизации управления при помощи информационной модели, имеющей форму базы данных (БД).База данных – это совокупность компьютерных данных о предметной области и сопровождающей их схемы, которая определяет адреса и форматы всех элементов данных, устанавливает связи между ними и предписывает правила записи/чтения данных [8],[9].

Идеальныйм метауровень отображает смысловое взаимодействие пользователей, обращающихся к БД для записи или считывания данных. Здесь в терминах предметной области формулируются цели управления и круг задач, для решения которых создана база данных.

Материальный метауровень отображает правила доступа пользователей к данным в соответствии с их адресами, форматами, правилами использования, корректировки и защиты. Взаимодействие пользователей с базой данных должен поддерживаться специальными языками для формирования запроса доступа к нужным данным. Запросы реализуются информационно-поисковыми системами.

Физическая среда взаимодействия обеспечивает сохранение данных в компьютерной памяти и в зависимости от используемого физического принципа сохранения требует того или иного количества пространственных, временных и энергетических ресурсов.

Заключение. Обобщенная модель информационного взаимодействия может быть использована в различных предметных областях. Изучение информационного взаимодействия позволяет комплексно подходить к решению многих практических задач и как следствие выбирать эффективные решения по организации информационного взаимодействия в интересах той или иной предметной деятельности, где реализуется данная модель.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Двухуровневая модель информационного взаимодействия//Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013. С 184-185.
2. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности // Геополитика и безопасность. 2014. № 1. С. 69–77.
3. Шеннон К.Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – 830 с.
4. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Модель физических характеристик сигналов // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)», Санкт-Петербург, 2013. С. 65–66.
5. Советов Б.Я., Цехановский В.В. Информационные технологии. Изд-во «Юрайт», М.: 2012. – 263 с.
6. Татарникова Т.М. Защищенные корпоративные сети: задачи по защите информации. – СПб: РГГМУ, 2012. – 113 с.
7. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель обработки клиентских запросов//Телекоммуникации. 2013 №9. С. 42-48.
8. Советов Б.Я., Цехановский В.В., Чертовской В.Д. Интеллектуальные системы и технологии. – М.: Академия, 2013. – 320 с.
9. Татарникова Т.М. Управление данными. – СПб.: СПбГУТ, 2006. – 83 с

УДК 502.084

СОЦИАЛЬНАЯ ИММУННАЯ СИСТЕМА И ИММУНОКОМПЬЮТИНГ

Владислав Станиславович Блюм, Вадим Петрович Заболотский,
Санкт-Петербургский институт информатики и автоматизации РАН,
СПИИРАН, Россия, Санкт-Петербург, 14-я линия ВО, д. 39,
e-mails: vlad@blum.spb.su, lai@iias.spb.su.

Аннотация: Статья посвящена анализу тенденций в развитии информатизации здравоохранения. Анализ аналогий в структуре и функциях иммунной системы и системы здравоохранения указывает на то, что полнота и достоверность первичной медицинской информации есть базовое условие

информационной безопасности пациентам. Ни одна электронная медицинская запись не может быть оставлена без внимания социальной иммунной системы. Каждая электронная медицинская запись должна должна быть включена в программную обработку в федеральном центре с целью оперативного управления ресурсами здравоохранения и минимизации ущерба от дефектов оказания медицинской помощи.

Ключевые слова: *информатизация здравоохранения; дефекты оказания медицинской помощи; интегрированная электронная медицинская карта*.

SOCIAL IMMUNE SYSTEM AND IMMUNOCOMPUTING

Blum Vlad, Zabolotski Vadim,
The St. Petersburg, SPIIRAS,
Russia, St. Petersburg, 14 line, 39,
e-mails: vlad@blum.spb.su, lai@iias.spb.su.

Abstract: This article analyzes the trends in the development of health information. Analysis of similarities in the structure and function of the immune system and the health system indicates that the completeness and accuracy of the primary medical information have a basic condition of information security to patients. None of the electronic medical record can not be disregarded social immune system. Each electronic medical record should be included in the software processing in the federal center with the aim of operative management of health resources and to minimize the damage caused by defects of care.

Keywords: *Computerization of health; defects care; integrated electronic medical record.*

Введение

Несмотря на великое множество больниц, поликлиник, машин скорой помощи и страховых компаний, система здравоохранения, в первую очередь, это конечное множество активных и пассивных лечебно-диагностических процессов, число которых на годичном интервале равно, как минимум, числу граждан страны. Эта, всё охватывающая, особенность социальной системы охраны здоровья в жизни общества позволяет говорить об её глубокой аналогии с ролью, которую играет иммунная система в жизни человеческого организма.

Пока далеко не осознана роль и значение информационных технологий, которые стремительно проникают в существо протекающих в обществе лечебно-диагностических процессов и усугубляют указанную аналогию.

Социальная система охраны здоровья, решая свои целевые задачи, неуклонно увеличивает объём производимой информации. При этом её структура и функциональные возможности не поспевают за информационным наполнением, что не позволяет качественно управлять целями и ресурсами лечебно-диагностических процессов и кардинально уменьшить число дефектов оказания медицинской помощи.

Ежегодно система здравоохранения страны производит, только клинической информации, более пяти терабайт, для традиционного, бумажного хранения такого объёма информации требуется ежегодно заготавливать более 20 тысяч деревьев [1].

Возникающие повсеместно электронные персональные медицинская записи (ЭПМЗ) – это новые базовые элементы в потоке клинической информации, современные кирпичики в истории болезни, в которых должны фиксироваться все события в клинической сфере системы здравоохранения. В результате, стала формироваться новая, гораздо более динамичная структура – электронная медицинская карта (ЭМК), которая пока мирно сосуществует с традиционной бумажной историей болезни. В настоящей статье мы не будем обсуждать проблемы этого временного сосуществования.

Противоречие между способом хранения персональных медицинских записей и многократно возросшим потоком телеметрической информации о здоровье пациента давно стало очевидным тормозом в повышении эффективности оказания медицинских услуг. И дело не только в нерациональном использовании лесных ресурсов. Слава богу, в России леса много и ресурс этот медленно, но можно восстанавливать.

Главное противоречие состоит в том, что возникновение в памяти компьютера такого объекта как электронная персональная медицинская запись (ЭПМЗ) открывает новые, до конца не осознанные, возможности качественного повышения скорости оценки состояния здоровья не только отдельного гражданина, но и региона, и всей страны, а на этой основе эффективно управлять ограниченными ресурсами здравоохранения.

Основной тезис, требующий осознания, заключается в том, что открывшаяся возможность интегрирования ЭПМЗ требует постановки и решения новых, ранее не достижимых, задач информационной поддержки врачебной деятельности с целью уменьшения числа дефектов оказания медицинской помощи, раннего обнаружения врачебных ошибок, а, в конечном счёте, качественного повышения эффективности управления здравоохранением.

С этих позиций предлагается рассмотреть структуру и технологии использования электронной персональной медицинской записи, в которой фиксируется клиническая информация о результатах взаимодействия пациента с системой охраны здоровья, опираясь на аналогию с функциями иммунной системы (системы охраны здоровья) человека.

Эволюция систем охраны здоровья. Аналогии верхнего уровня

Только два типа биологических систем – нервная и иммунная – обладают способностями «интеллектуальной» обработки информации, включая память, обучение, распознавание и принятие решений в заранее незнакомых ситуациях.

В процессе эволюции живых существ возникли многоклеточные организмы. По мере усложнения их строения происходила специализация функций разных клеток и состоящих из них органов: пищеварения, дыхания и других. На определенном этапе эволюции в многоклеточном организме появились клетки, призванные защищать организм от микробов-паразитов. Постепенно сформировалась особая система органов и клеток, обеспечивающих приём и обработку информации о вторжениях, которая получила название иммунной системы. Клетки, входящие в состав иммунной системы, были названы иммунокомпетентными.

Аналогичный, но гораздо более быстрый, эволюционный процесс привёл к формированию современной системы охраны здоровья, в которой роль иммунокомпетентных клеток общества играют профессиональные обработчики клинической информации: дипломированные (лицензированные, сертифицированные, аттестованные) врачи и лицензированные диагностические лаборатории.

Иммунная система осуществляет защиту с помощью двух типов лечебно – диагностических процессов: неспецифического (врожденного, естественного) и специфического (приобретенного) иммунитета [4–23]. Это две стадии единого технологического процесса защиты организма. Неспецифический иммунитет выступает как первая линия защиты и как заключительная ее стадия. Система приобретенного иммунитета выполняет промежуточные функции специфического распознавания и запоминания болезнетворного агента (или чужеродного вещества), после чего подключаются мощные средства врожденного иммунитета для заключительного этапа борьбы с вторжениями.

Система здравоохранения базируется на трёх технологических линиях единого лечебно-диагностического процесса – это система скорой медицинской помощи, система поликлинической медицинской помощи и система стационарной медицинской помощи.

В попытке провести параллели между указанными технологиями охраны здоровья в человеке и обществе, можно говорить о соответствии функций системы неспецифического иммунитета функциям системы поликлинической медицинской помощи, в то время как функции специфического иммунитета ближе к функциям стационарной медицинской помощи.

В наших знаниях о работе иммунной системы пока остаются открытыми вопросы:

– Каким образом защитные клетки, циркулирующие в крови или осевшие в органах и тканях иммунной системы, отдаленных от мест уязвимости организма, получают и воспринимают сигнал опасности микробной агрессии?

– Как обеспечивается строгая последовательность включения отдельных типов клеток в борьбу с инфекцией?

– Откуда узнает иммунная система, какие именно защитные механизмы следует использовать при данной инфекции?

Ответы на аналогичные вопросы в работе системы общественного здравоохранения с необходимостью зафиксированы в соответствующих директивных документах.

На объективность рассматриваемых аналогий указывает установившееся соотношение числа врачующих элементов и общего числа потенциальных пациентов в человеческом организме и обществе. Общее число клеток нашего организма составляет десять в четырнадцатой степени. Число же врачующих клеток, лимфоцитов, порядка десять в двенадцатой степени. По данным ВОЗ [24] в развитых системах здравоохранения сложилось соотношение числа врачей к числу пациентов, как 1 к 300.

Аналогии в структуре и составе эффекторов

Информационные каналы

Информационные каналы иммунной системы построены на основе магистралей крови и лимфы. Эти каналы носят всеохватывающий характер и имеют общую длину более 95 тысяч километров. Тем самым обеспечена поразительная плотность каналов обмена информацией. В нашем обзоре [2] отмечен замкнутый характер и высокая интенсивность циркуляции белковых носителей информации.

Опираясь на закон Маррея, можно говорить о качественной смене метода циркуляции данных внутри органа и вне его. Указанный порог пропускной способности информационных каналов позволяет выделить в организме порядка 25 тысяч модулей биомассы, в которые оперативно доставляется информация системой кровообращения по множеству входящих и исходящих каналов.

С большим основанием можно утверждать, что всеохватывающий характер и интенсивность информационного обмена позволяют эффективно управлять процессом борьбы с вторжениями, мобилизуя для этого ограниченные ресурсы организма.

До последнего времени, говорить о единой схеме циркуляции клинической информации в нашей стране не приходилось.

В России десятки тысяч ЛПУ, процесс встраивания которых в единую информационно-телекоммуникационную структуру здравоохранения только начался.

Недооценка роли и значения телекоммуникационной инфраструктуры в системе охраны здоровья по-прежнему очень велика.

Создание федерального и региональных центров обработки медицинской информации, а также включение в сеть всех без исключения источников клинической информации сделает аналогии рассматриваемых систем охраны здоровья гораздо более очевидными.

Система поверхностей вторжений

Организм позвоночного животного, в рамках которого имеет смысл понятие «иммунная система», обладает огромной и непрерывной, с позиций топологии, поверхностью контактов с внешним миром. Речь идет о поверхностях кожного покрова, органов дыхания и органов пищеварения. Ограниченное указанной непрерывной поверхностью 3-х мерное пространство может быть названо пространством иммунитета, защитой от вторжений в которое занимается иммунная система.

Социальная иммунная система России также имеет огромную внешнюю поверхность вторжений, которая складывается из сухопутной, морской и воздушной границ нашей страны. Виртуальная непрерывность этой границы формируется в головах работников специальной структуры, называемой Росздравнадзор.

Центральные органы

К первичным центральным органам иммунной системы относят вилочковую железу (тимус) и костный мозг [3]. Оба эти органа связаны с производством и обучением необходимого числа и разнообразия эффекторов (основных клеток исполнителей функций) иммунной системы. Именно в этих органах непрерывно и оперативно выполняется анализ и обобщение опыта «клинической» работы системы охраны здоровья.

Аналогичную роль в охране общественного здоровья играют система медицинского образования и система управления в форме министерства здравоохранения и его региональных подразделений. Однако о владении этими органами полной и достоверной клинической информацией говорить пока не приходится, и, следовательно, рассчитывать на эффективное управление ресурсами тем более не приходится.

Периферические органы

К периферическим органам иммунной системы относятся селезенка, лимфатические узлы, миндалины, а также ассоциированная с кишечником и бронхами лимфоидная ткань. К моменту рождения они еще практически не сформированы, поскольку не контактировали с антигенами. Лимфопоэз в них осуществляется лишь при наличии антигенной стимуляции. Периферические органы иммунной системы заселяются В- и Т-лимфоцитами из центральных органов иммунной системы, причем каждая популяция мигрирует в свою зону – тимусзависимую и тимуснезависимую. После контакта с антигеном в этих органах лимфоциты включаются в рециркуляцию, поэтому ни один антиген не остается незамеченным лимфоцитами [3].

В социальной иммунной системе (системе здравоохранения) также сформировались два класса объектов, выполняющих задачу обнаружения, анализа и нейтрализации вторжений (болезней). Это дипломированные врачи и лицензированные диагностические лаборатории.

Общее число врачей в нашей стране составляет около 650 тысяч, а число лабораторий порядка 30 тысяч. Как уже отмечалось, соотношение общего числа лимфоцитов к общему числу клеток человеческого организма соответствует соотношению информационных источников медицинской (клинической) информации к общему числу потенциальных пациентов, граждан страны.

Указанные источники первичной медицинской информации организуются в различные формы периферических структур, начиная от индивидуального предпринимателя и заканчивая больницами, госпиталями и медицинскими центрами.

Отмечая аналогии в составе и относительной численности эффекторов рассматриваемых систем охраны здоровья, следует подчеркнуть, что для выявления функционального подобия периферических структур потребуется с одной стороны, более глубокое понимание функций каждого отдельного периферического органа иммунной системы, а с другой стороны, развитие и оптимизация информационной инфраструктуры циркуляции клинической информации в системе здравоохранения.

Аналогии в потоках клинической информации

Функции иммунной системы, в современным понимании, неразрывно связаны с понятием антигена, которым идентифицируются все возможные вторжения, нарушающие функциональную целостность организма [3].

Антигены – (от анти и греч. génos – рождение, происхождение), высокомолекулярные коллоидные вещества, которые при введении в организм животных и человека вызывают образование специфических реагирующих с ними антител.

Непременным условием антигенности является отличие антигенов от веществ, имеющихся в норме в организме реципиента. К антигенам относятся прежде всего чужеродные белки, некоторые полисахариды (большей частью бактериального происхождения), комплексы белков с разнообразными химическими соединениями. Антигены бывают корпускулярные (например, взвеси бактерий), дающие с антителами реакцию агглютинации (склеивания), и растворимые (например, токсины), дающие реакцию преципитации (осаждения).

В основе реакции иммунной системы на вторжение антигена лежит производство специфических антител, наряду с реакцией системы комплемента и фагоцитозом.

Антитела (antibodies) – белки относящиеся к подклассу гамма-глобулинов, образующиеся в организме при попадании в него некоторых чужеродных веществ (антигенов) и обладающие способностью избирательно соединяться с теми же антигенами или (в меньшей степени) со сходными с ними по строению веществами, вызывая тем самым иммунный ответ организма [3].

Антитела реагируют только с теми антигенами, которые индуцировали их синтез. Изменения химической или физической структуры антигенов приводят к образованию иных, видоизмененных антител. Такое прямое соответствие между антигенами и антителами известно под названием специфичности.

Форма молекулы антитела и распределение электрического заряда по ее поверхности делают ее способной связывать антиген, комплементарный ей по форме и распределению заряда.

В борьбе с антигенами и в производстве антител (средств лечения с вторжениями) задействованы следующие основные клетки (эффекторы) иммунной системы: фагоциты и лимфоциты.

Фагоциты, получили своё название от греческого phago – «есть» и cyt – «клетка». Кроме кровотока, главная территория фагоцитов в организме — это селезенка, костный мозг, лимфатические узлы, альвеолярные мешочки в легких (легочные альвеолы), брюшина (мембрана брюшной стенки), печень, соединительная ткань и центральная нервная система.

Фагоциты не только выполняют роль санитаров-мусорщиков в организме, но и, обнаружив антиген, сигнализируют об этом другим участникам иммунного процесса.

Лимфоциты составляют основную массу клеточных элементов лимфоидной ткани, 95% клеток лимфы и 30% общего числа лейкоцитов крови.

Обратим внимание на тот факт, что количество лимфоцитов в иммунной системе имеет, по крайней мере, один порядок величины, что и число нейронов в нервной системе. Лимфоциты среди прочих клеток нашего тела, распространяемых по крови и лимфе, имеют наибольшие концентрации в селезенке, лимфоузлах, тимусе и костном мозге. Но их практически нет в мозге. [THE IMMUNE SYSTEM Nobel lecture, 8 December 1984 by NIELS K. JERNE]

Специфическое взаимодействие антител с соответствующими антигенами приводит к образованию комплексов антиген–антитело (иммунных комплексов).

Решающую роль в функции иммунного ответа играют, так называемые, Т- и В-лимфоциты [4–3].

Т-лимфоциты держат весь иммунный ответ под контролем, не допуская чрезмерной активации отдельных иммунокомпетентных клеток, которая чревата осложнениями. Инструментами такого контроля служат цитокины, способные не только активировать (усиливать), но и подавлять (ингибировать) функции других клеток.

Защита организма, осуществляемая с помощью Т-клеток, называется клеточным иммунитетом, так как в ее основе лежит взаимодействие отдельных клеток с антигенами.

Контакт рецепторов В-лимфоцитов со специфическим антигеном и связывание определенного его количества стимулируют рост этих клеток и последующее многократное деление; в результате образуются многочисленные клетки двух разновидностей: плазматические и «клетки памяти». Плазматические клетки синтезируют антитела, выделяющиеся в кровоток.

Клетки памяти являются копиями исходных В-клеток; они отличаются большой продолжительностью жизни, и их накопление обеспечивает возможность быстрого иммунного ответа в случае повторного попадания в организм данного антигена.

Антитела, вырабатываемые В-клетками и поступающие в кровь и другие жидкости организма, относят к факторам гуморального иммунитета (от лат. humor – жидкость).

Для обмена информацией в процессе иммунного ответа и его регулирования клетки-эффекторы иммунной системы используют, производимые ими небольшие белки – цитокины [3].

При физиологическом состоянии в норме, спектр цитокинов узок, но при стрессе, воспалении, повреждении, опухолеобразовании и др. расширяется количественный и качественный состав цитокинов, обладающих как местной, так и дистантной активностью.

Цитокины самоорганизуются в цитокиновые сети с разветвленными многоуровневыми прямыми и обратными связями. Благодаря этому передаваемая через них клеткой информация содержится не в отдельно взятом цитокине, но в их ансамблях. Регуляторные влияния при этом становятся согласованными и выверенными. Действия однонаправленного характера мультиплицируются, а разнонаправленного уравновешиваются.

Работа иммунокомпетентных клеток (лимфоцитов и фагоцитов), их циркуляция в кровеносном русле, а также циркуляция произведенных ими специализированных белков (антител и цитокинов), в ответ на вторжения антигенов, образуют непрерывный поток «клинической информации». От объёма и интенсивности этого потока зависит объём ресурсов, которые включает организм на борьбу с болезнью.

Поток клинической информации в системе здравоохранения в ближайшей перспективе будет формироваться только из электронных персональных медицинских записей, которые производят врачи и диагностические лаборатории.

ЭПМЗ диагностической лаборатории в клинической сфере здравоохранения выполняет информационную роль аналогичную роли антигена в организме человека.

ЭПМЗ врача, в зависимости от наличия или отсутствия в ней схемы лечения, играют в лечебно-диагностическом процессе роль иммунного комплекса (антиген-антитело), либо роль антигена (признаков конкретной болезни), для которого ещё не определено средство нейтрализации.

<ЭПМЗ ВРАЧА>::= <время сеанса>< идентификатор ВРАЧА> < идентификатор ПАЦИЕНТА><документ ВРАЧА>

<документ ВРАЧА>::= <жалобы пациента><анамнез><диагноз><план лечения><назначения>

Грамматические категории <время сеанса>, <идентификатор ВРАЧА> и <идентификатор ПАЦИЕНТА> имеют абсолютные и уникальные значения, которые не зависят от контекста. В то время, как категория <документ ВРАЧА> и все её составляющие имеет очевидную контекстную зависимость от предыстории, предыдущих ЭПМЗ в истории болезни данного пациента.

Социальный характер отдельной ЭПМЗ пока до конца не осознан. Он проявляется весьма опосредовано и интегрально в результатах обработки статистических медицинских данных, на формирование и обслуживание которых работает специализированная и довольно громоздкая инфраструктура в системе здравоохранения.

При этом, говорить об оперативном управлении ресурсами охраны здоровья в ответ на выявленные «антигены» в масштабах региона, а тем более страны, пока не приходится.

Тоже самое, можно сказать и о выявлении дефектов оказания медицинской помощи, которые фиксируются в ЭПМЗ – «иммунных комплексах», но обнаруживаются, как правило, слишком поздно.

Аналогии в функциях систем охраны здоровья

Иммунный ответ в организме человека включает две важнейшие подфункции: функцию иммунизации и функцию апоптоза.

Функция иммунизации, в свою очередь, имеет две составляющие:

1. Система данных и алгоритмов, которые «вшиты» в иммунную систему и передаются по наследству. Это то, что называется неспецифическим (врожденным) иммунитетом и обуславливает однотипные (стандартные) реакции на чужеродные вторжения.

2. Система данных и алгоритмов, которые формируются и настраиваются в процессе работы иммунной системы. Это происходит всякий раз, когда происходит вторжение вещества, которое не может быть нейтрализовано и выведено организмом по стандартной схеме. В этом случае реакцию обеспечивает специфический иммунитет. Он приобретается в результате контакта организма с антигеном; имеет приспособительное значение и характеризуется формированием иммунологической памяти. Первое взаимодействие антигена (бактерии или вируса) с лимфоцитом вызывает реакцию, названную первичным иммунным ответом, в ходе которого лимфоциты начинают развиваться (пролиферировать) в виде клонов, претерпевая затем дифференцировку: некоторые из них становятся клетками памяти, другие превращаются в зрелые клетки, продуцирующие антитела. Главные особенности первичного иммунного ответа – существование латентного периода до появления антител, затем выработка их лишь в небольшом количестве. Вторичный иммунный ответ развивается при последующем контакте с тем же самым антигеном. Основная особенность – быстрая пролиферация лимфоцитов с дифференцировкой их в зрелые клетки и быстрая выработка большого количества антител, которые высвобождаются в кровь и тканевую жидкость, где могут встретиться с антигеном и эффективно побороть болезнь.

В общественной системе охраны здоровья функция иммунизации также поддерживается двумя технологическими линиями: поликлинической медицинской помощью и стационарной медицинской помощью, которые заметно отличаются по степени применения стандартных схем лечения пациентов.

Апоптоз – это активная форма гибели клетки, являющаяся результатом реализации ее генетической программы или ответом на внешние силы и требующая затрат энергии и синтеза макромолекул de novo, проявляющаяся в уменьшении ее размера, конденсации и фрагментации

хроматина, уплотнении наружной и цитоплазматических мембран без выхода содержимого клетки в окружающую среду.

Функция апоптоза необходима для понимания иммунного гомеостаза. Гибель части клеток в пределах организма является закономерным и необходимым явлением, и само существование многоклеточного организма подразумевает баланс жизни и смерти на уровне составляющих его клеточных популяций.

Функция апоптоза в социальной иммунной системе проявляется в её целенаправленных усилиях по увеличению продолжительности жизни пациентов и повышения качества их жизни при наличии выявленных хронических заболеваний.

Системы охраны здоровья, как системы информационной безопасности

Работа иммунной системы человека в полном объеме начинается еще в утробе матери и выполняется без перерывов и выходных в течение всей жизни организма.

Взрослый человеческий организм – это совместное проживание порядка 10^{14} клеток, каждая из которых является носителем идентификатора организма – кода ДНК.

При этом каждая клетка организма является объектом контроля собственной иммунной системы – системы информационной безопасности, которая для каждой клетки решает задачи целостности, конфиденциальности и доступности информации на основе анализа полного, достоверного и доступного для обработки потока клинической информации.

Социальная иммунная система – система здравоохранения – также задействована в жизни каждого гражданина страны с момента его рождения до момента смерти. Теоретически и законодательно забота о здоровье каждого гражданина является непрерывно выполняемой функцией государственной системы охраны здоровья.

В нашей стране проживает более 10^{8} граждан, каждый из которых с момента рождения обладает персональной медицинской картой. В ближайшей перспективе эта карта примет вид электронной медицинской карты (ЭМК) и непременно приобретёт уникальный идентификатор, который будет сопровождать пациента от рождения до смерти.

Современный этап информатизации здравоохранения открывает реальные перспективы непрерывного учёта и оперативного мониторинга работы источников клинической информации, формирования полной, достоверной и доступной для оперативной компьютерной обработки электронных медицинских карт, а также их хранение на интервале всей жизни пациента.

Запуск неспецифического иммунного ответа

Задача информационной целостности клетки решается средствами самой клетки (дублирование информации, защитные свойства мембраны, включение апоптоза и т.п.), а также средствами иммунной системы. Целостность (здоровье) клетки и её соответствие родительскому организму контролируют система комплемента (комплекс белков, постоянно присутствующих в крови) и различные типы лейкоцитов. Для этого используется, как на современных самолетах, не сложный, но секретный прибор «свой-чужой». С большой вероятностью можно сказать, что в основе алгоритма данного прибора лежит уникальный для данного организма код ДНК, которым обладает, как контролируемая так контролирующая клетки.

Очевидно, что инициатива в диалоге «свой-чужой» принадлежит контролируемой клетке. Сигналы о нарушении целостности клетки в многоклеточном организме формируются внутри каждой клетки.

К сожалению, интенсивность таких сигналов от клеток злокачественных опухолей недостаточна для эффективной работы иммунной системы.

В социальной системе охраны здоровья контроль самочувствия также является, большей частью, заботой самого гражданина. Обнаружение им значительных нарушений в состоянии своего здоровья превращаем гражданина в пациента и активизирует лечебно-диагностический процесс.

Можно с уверенностью говорить, что система здравоохранения запускает лечебно-диагностический процесс в отношении конкретного гражданина в момент его рождения и завершает вскоре после его смерти, чередуя его активные и пассивные фазы.

Пациенты с типовыми, известными, не опасными для жизни заболеваниями обслуживаются семейными врачами, амбулаториями и поликлиниками. Также, как иммунная система, система здравоохранения именно в этом звене грешит наибольшим числом дефектов оказания медицинской помощи, что часто приводит к потере драгоценного времени и превращает патологический процесс в необратимый.

Запуск специфического иммунного ответа

Пусковым моментом для включения специфического иммунного ответа организма является взаимодействие Т-лимфоцита с антигенпрезентирующей клеткой (АПК) [3]. Инициатива АПК проявляется отправкой сообщений-цитокинов с целью привлечь внимание к объекту вторжения со стороны специализированных специалистов – Т-лимфоцитов.

< АПК >&< молекула МНС II >&<антиген>→(ИЛ-2)→<Th0 > – так формально можно описать встречу антигена с незрелым (наивным) Т-лимфоцитом [3].

Возможны и иные варианты встреч антигена с лимфоцитами и каждая из них имеет свое продолжение. В частности, встреча антигена с В-лимфоцитом, как уже отмечалось, может привести к открытию целого фармакологического предприятия по производству необходимого количества эффективного лекарства – специфических антител. В-лимфоциты, кроме того, создают базу иммунологической памяти организма.

В любом случае, запуск специфического иммунного ответа связан с мобилизацией ресурсов организма и привлечением специальных, узкоспециализированных средств борьбы с вторжениями (болезнями).

Образом специфического иммунного ответа в социальной системе охраны здоровья выступает технология стационарного лечения, которая получает пациентов из систем скорой и поликлинической помощи.

Именно в этом звене системы здравоохранения сконцентрированы основные ресурсы и новейшие технологии оказания медицинской помощи. В системе госпитальной помощи достигается максимальная специализация и глубина лечебно-диагностического процесса. На этом же звене лежит основная нагрузка по проведению клинических испытаний новых медикаментозных средств и методов лечения.

Однако, консерватизм современной технологии стационарного лечения, информационная замкнутость каждого отдельного стационара вступают во всё большее противоречие с необходимостью перехода на качественно иной уровень обмена клинической информацией для эффективного управления ограниченными ресурсами здравоохранения, повышения скорости внедрения прогрессивных технологий лечения, наконец, для раннего обнаружения дефектов оказания медицинской помощи. Указанное противоречие, на наш взгляд, является основным сдерживающим фактором в повышении результативности лечебно-диагностических процессов.

Иммунокомпьютинг

Иммунокомпьютинг, как новое направление информатики, возникло на основе анализа и попыток построения математических моделей, основанных на принципах обработки информации молекулами белков и иммунными сетями [2]. Однако, больших успехов данное научное направление пока не достигло, что можно объяснить недостаточной глубиной наших знаний о процессе обнаружения и ликвидации вторжений антигенов в нашем организме.

Основной, общепризнанный, принцип работы иммунной системы – это свободное, но целенаправленное связывание базовых элементов (*протеинов*) в рамках *иммунной сети*. При этом принципиальными факторами достижения системных целей являются замкнутый характер и высокая концентрация информационных каналов иммунной системы, а также их высокая и управляемая пропускная способность, обеспечивающая необходимый уровень циркуляции информации.

На наш взгляд, начало качественных изменений в информационной инфраструктуре здравоохранения и внедрение компьютерных технологий в сферу сбора и обработки клинической информации позволяет во всё большей степени рассматривать клиническую составляющую системы здравоохранения, как социальную иммунную систему.

При этом роль математических моделей для прогнозирования и анализа различных информационных процессов во вновь создаваемой социальной иммунной системе трудно переоценить.

Поэтому, с большим основанием можно утверждать, что в предмет исследований иммунокомпьютинга (теории искусственных иммунных сетей) должны войти:

1. Исследование структуры и информационных свойств электронной персональной медицинской записи.
2. Исследование структуры, пропускной способности и моделирование интерфейса сбора клинической информации, который образуется в результате деятельности информационных источников: врачей и диагностических лабораторий.
3. Исследование необходимых и достаточных условий формирования полного, достоверного и доступного для компьютерной обработки потока клинической информации.

Дальнейшее развитие иммунокомпьютинга и его аппаратных реализаций в сфере здравоохранения может привести к следующим прорывам в области обработки клинической информации:

– Иммунокомпьютинг способен преодолеть разобщенность в создании многочисленных медицинских систем, выступая в качестве единой методологической базы.

– Иммунокомпьютинг обеспечивает наиболее адекватное компьютерное моделирование социальной иммунной системы.

– Иммунокомпьютинг дает возможность системам диагностики обрабатывать громадные объемы данных в режиме реального времени, обеспечивая при этом надлежащее обнаружение и предсказание ошибок и критических ситуаций.

– Иммунокомпьютинг может способствовать развитию области информационной безопасности за счет обеспечения математически строгого базиса для разработки самообучающихся систем безопасности, способных противостоять заранее неизвестным вторжениям и обеспечить программно-аппаратную реализацию таких систем.

Заключение

Целью статьи является попытка обратить внимание на три аспекта в развитии информатизации здравоохранения.

1. Опираясь на приведённые аналогии, можно утверждать, что презумпция ценности отдельной человеческой жизни превыше всякой болтовни о защите персональных данных в потоке клинической информации.

2. Ни одна электронная персональная медицинская запись не может быть оставлена без необходимой и достаточной реакции социальной иммунной системы.

3. Каждая электронная персональная медицинская запись должна стать объектом программной обработки не только в контексте полной персональной электронной медицинской карты в конкретном ЛПУ, но также и в региональном, и в федеральном центре для оперативного управления ресурсами здравоохранения и минимизации ущерба от дефектов оказания медицинской помощи.

СПИСОК ЛИТЕРАТУРЫ

1. Блюм В.С., Заболотский В.П. Мысленный эксперимент по организации учета и обработки информационных медицинских услуг. Врач и информационные технологии, №4 2009. С.27–35
2. Tarakanov A. O., Skormin V. A., Sokolova S. P. Immunocomputing: Principles and Applications. New York.: Springer, 2003, 230 p.
3. Блюм В.С., Заболотский В.П. Иммунная система и иммунокомпьютинг. Математическая морфология. Электронный математический и медико-биологический журнал (том 6 выпуск 4, 2007). Зарегистрировано 29.01.2008 под номером 0420700004/0039.
4. Абелев Г.И. Основы иммунитета // Соросовский Образовательный Журнал. 1996. №5. с.4–10.
5. Иммунология. Под ред. У. Пола. М.: Мир, 1988. Т. 1–3.
6. Хаитов Р.М., Игнатьева Г.А., Сидорович И.Г. Иммунология. – М., Медицина, 2000.
7. Клиническая иммунология и аллергология Под ред. Г. Лолора-младшего, Т. Фишера, Д. Адельмана. Пер. с англ. – М., Практика, 2000, – 806 с.
8. Ярилин А.А. Основы иммунологии. – М., Медицина, 1999.
9. Галактионов В.Г. Графические модели в иммунологии. М.: Медицина, 1986.
10. Зарецкая Ю.М., Хамагонова Е.Г., Губарев М.И. Иммунология и иммуногенетика человека, Триада, Москва, 2002. 128 с.
11. Peakman M. and Vergani D. Basic and clinical immunology. NY: Churchill Livingstone, 1997. – 338 p.
12. Janeway Ch., Travers P. Immunobiology. 3 ed. Curr. Biol. Ltd., 1997.
13. Новиков Д.К. Медицинская иммунология. ВГМУ; 1998.
14. Кудрявцев И.В., Полевщиков А.В. Эволюция каскада комплемента: ранние этапы // Цитокины и воспаление. 2005. Т. 4, №1. С. 11–21.
15. Logic (ISMVL '97).
16. Tang T. Proceedings of the 27th International Symposium on Multiple-Valued.
17. Ройт А. Основы иммунологии (пер. с англ.). М.: Мир, 1991. 328 с.
18. Кетлинский С.А., Симбирцев А.С., Воробьев А.А. Эндогенные иммуномодуляторы. СПб.: Гиппократ, 1992. 256 с.
19. Фрейдлин И.С. Система мононуклеарных фагоцитов. М.: Медицина, 1984. 272 с.
20. Маянский А.Н., Маянский Д.Н. Очерки о нейтрофиле и макрофаге. Новосибирск: Наука, 1989. 340 с.
21. Албертс Б., Брей Д., Льюис Дж., Рэфф М., Робертс К., Уотсон Дж. Молекулярная биология клетки. М.: Мир, 1994. Т. 2. С. 287–301.
22. Молекулярная биология. Структура и биосинтез нуклеиновых кислот / Под ред. акад. А.С. Спирина. М.: Высшая школа, 1990. С.44–73.
23. Льюин Б. Гены. М.: Мир, 1987. С. 396–431.
24. Мировая статистика здравоохранения. / http://www.who.int/whosis/whostat/RU_WHS10_Full.pdf

УДК 51.007.004

СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИЗВЛЕКАЕМОЙ СПЕЦИАЛЬНЫМ ОБРАЗОМ ИНФОРМАЦИИ

Копыльцов Антон Александрович,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mail: antonkop@gmail.com.

Аннотация: В статье предлагается обобщенный алгоритм обработки слабо формализованной информации, поступающей от технических систем. Алгоритм позволяет осуществлять поддержку принятия решений в слабо формализованных областях.

Ключевые слова: *алгоритм; слабо формализованная информация; конфиденциальность данных; поддержка принятия решений*

THE SAVE OF CONFIDENTIALITY DATA IN DECISION SUPPORT BASED ON EXTRACTS SPECIALLY INFORMATION

Kopyltsov Anton Alexandrovich,
St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
e-mails:antonkop@gmail.com.

Abstract: In this paper we propose a generic algorithm for processing weakly formalized information from technical systems. The algorithm allows for decision support in weakly formalized areas.

Keywords: *algorithm; weakly formalized information; confidentiality of data; decision support*

В связи с развитием техники используется большое количество технических систем, с которых осуществляется сбор разнообразной информации с помощью различных датчиков. Информация, поступающая от технических систем, весьма разнообразна. Это могут быть видеокамеры, датчики звука и ультразвука, тактильные датчики, датчики, регистрирующие температуру, давление, вибрацию, ионы, направление силы тяжести и многое другое. Количество таких датчиков, установленных на технической системе, может измеряться сотнями. Поступающая информация часто является слабо формализованной, содержит искажения, помехи, шумы. Обработка такой информации, с целью подготовки принятия решений, осуществляется различными способами. Каждый из подходов имеет свои преимущества и недостатки. Однако, системы, которые позволяли бы это делать удовлетворительно, до сих пор не созданы. Сложность решения этой проблемы состоит в том, что с развитием техники объем слабо формализованной информации, поступающей от технических систем, с одной стороны, существенно возрастает, а с другой стороны, интервалы времени, в течение которых нужно принимать правильные решения, резко сокращаются. Таким образом, разработка моделей и алгоритмов обработки слабо формализованной информации, поступающей от технических систем, с целью поддержки принятия решений, актуальна.

При поддержке принятия решений важно сохранение конфиденциальности данных, поскольку при утрате важной информации решение может измениться. Построена система моделей и алгоритмов обработки слабо формализованной информации, в которой учитывается конфиденциальность данных, поступающих от технических систем и позволяющих осуществлять поддержку принятия решений.

Обзор интеллектуальных технологий и интеллектуальных вычислений показал, что методы обработки слабо формализованной информации интенсивно развиваются и наибольшего развития в последнее время получили эволюционные алгоритмы и различные их комбинации с нейронными, нечеткими, сетевыми и другими структурами, т.е., наибольшее развитие получили подходы, в основу которых заложены механизмы, реализованные в живых организмах.

Поэтому для решения проблемы обработки слабо формализованной информации, поступающей от технических систем, предлагается подход, в основу которого положены следующие способы хранения и обработки информации в живом организме:

1. Информация о каком-либо объекте в видео-, аудио- и других диапазонах хранится не в разных структурах мозга, а в одной и той же части, причем с течением времени эта зона нейронов расширяется (количество нейронов увеличивается), и в случае накопления информации количество связей между нейронами так же увеличивается.
2. Обработка какого-либо объекта в видео-, аудио- и других диапазонах, осуществляется одновременно не в разных структурах мозга, а в одной и той же части, независимо от вида информации.
3. Генерация новых знаний в мозге осуществляется путем сравнения вновь поступившей информации не со всей информацией, хранящейся в памяти, а только с определенным образом обработанной информацией, что позволяет существенно увеличить скорость обработки информации.
4. Внимание – основная функция мозга, обеспечивающая выживание организма в окружающей среде, т.е. обработка информации в мозге осуществляется с учетом приоритетов, что позволяет сократить объем хранящейся в памяти информации необходимой для принятия решений и увеличить скорость ее обработки.
5. Наблюдательность – важное свойство эволюции, позволяющее замечать повторяющиеся факты, т.е. выявлять периодические временные ряды, закономерности в событиях и явлениях, что позволяет увеличить скорость обработки информации при принятии решений.

На основе этих способов хранения и обработки информации в живом организме предлагается смешанная система поддержки принятия решений на основе смешанной системы обработки специальным образом информации и алгоритмов приоритетов, наблюдательности и генерации новой информации.

Такой подход позволяет:

– эффективно хранить информацию, путем хранения не всей информации, а только результатов ее специальной обработки;

– эффективно осуществлять обработку большого объема поступающей информации, путем варьирования приоритетами;

– выявлять повторяющиеся закономерности;

– генерировать новые знания, путем анализа имеющейся в памяти информации в виде результатов ее специальной обработки.

Система включает следующие подсистемы (Рис. 1) [1], [2], [3], [4], [5].

Подсистема сбора информации (1) предназначена для сбора информации, поступающей от технической системы.

Подсистема распознавания информации (2) предназначена для распознавания поступающей информации.

Подсистема классификации информации (3) – предназначена для классификации поступающей информации на некоторое количество классов (n), зависящее от конкретной задачи.

Подсистемы свертки информации (4-1, … , 4-i, … , 4-n) предназначены для обработки (свертки) информации в каждом из n классов.

Подсистемы оценивания достоверности информации (5-1, …, 5-i, …, 5-n) предназначены для оценивания достоверности поступающей информации в каждом из n классов, путем сравнения ее с ранее полученной информацией. Подсистемы оценивания безопасности информации (6-1, …, 6-i, …, 6-n) предназначены для оценивания безопасности поступающей информации в каждом из n классов.

Подсистемы установления связей (7-1, …, 7-i, …, 7-n).между вновь полученной информацией в каждом классе и ранее полученной информацией.

Подсистемы оценивания вероятности (8-1, …, 8-i, …, 8-n), с которой можно доверять полученной информации в каждом классе.

Подсистемы поддержки принятия решений в каждом классе (9-1, …, 9-i, …, 9-n) предназначены для поддержки принятия решений в каждом из n классов. Подсистема поддержки принятия обобщенных решений (10) предназначена для поддержки принятия решений на основе решений принятых в каждом из n классов.

Подсистема определения числа связей (11), подтверждающих правильность принято решения.

Подсистема выработки устойчивой реакции на поступающую информацию и ее закрепление (12) предназначена для выработки устойчивой реакции на многократно поступающую информацию и ее закрепление, путем сравнения полученной информации с ранее полученной информацией.

Подсистема поддержки принятия решений (13) предназначена для генерации решений. Подсистема хранения и генерации новой информации (14) предназначена для хранения информации поступившей ранее, сравнения вновь поступившей информации с информацией находящейся на хранении, генерации информации с последующей проверкой новая она или нет.

Система обработки слабо формализованной информации обеспечивает следующие функциональные возможности: оценивание достоверности поступающей информации, оценивание безопасности поступающей информации, оценивание вероятности, с которой можно доверять полученной информации, выработка устойчивой реакции на поступающую информацию и ее запоминание, поддержка принятия решений, генерация новой информации.

Работа системы включает следующие этапы (Рис.1).

Этап 1. Информация, поступающая от технической системы через совокупность различных датчиков, собирается в подсистеме «1».

Этап 2. Информация поступает из подсистемы «1» в подсистему «2», где осуществляется ее распознавание.

Этап 3. Из подсистемы «2» информация поступает в подсистему «3», где осуществляется ее классификация.

Этап 4. Информация, поступающая в каждый из n классов, подвергается в подсистемах «4-1», …, «4-i», …, «4-n» своей, присущей данному классу, обработке по определенному алгоритму (свертке). В итоге получается новая информация, обработанная специальным образом, присущим данному классу. В основу алгоритма свертки положен экспертный метод, разработанный ранее для оценки качества программных продуктов при недостатке информации [1], [2], [3], [4], [5].

Этап 5. После свертки в «4-1», …, «4-I», …, «4-n», осуществляется оценивание достоверности информации в подсистемах «5-1», …, «5-I», …, «5-n».

Этап 6. В подсистемах «6-1», …, «6-I», …, «6-n» осуществляется оценивание безопасности информации в каждом классе.

Этап 7. Установление связей между вновь полученной информацией в каждом классе и ранее полученной информацией, находящейся в «14», осуществляется в подсистемах «7-1», …, «7-I», …, «7-n».

Этап 8. Оценивание вероятности, с которой можно доверять полученной информации в каждом классе осуществляется в подсистемах «8-1», …, «8-I», …, «8-n» с помощью вероятностного алгоритма оценивания работоспособности системы наблюдения.

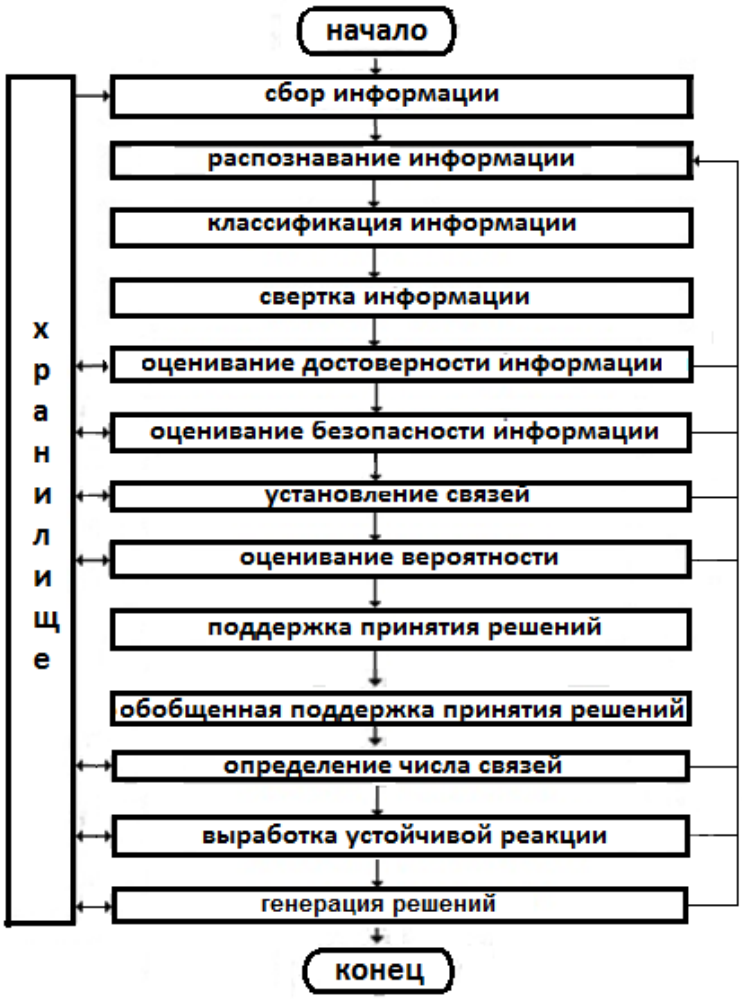


Рис. 1. Блок-схема обобщенного алгоритма обработки слабо формализованной информации.

Предполагается, что система наблюдения, от которой поступает различная информация, содержит модули: модуль зрения, модуль слуха, тактильный модуль, модуль вкуса и запаха, и др. При необходимости количество модулей легко может быть уменьшено или увеличено. Входными данными являются наименования неисправностей системы, наиболее часто встречающиеся при работе системы. Первоначально можно взять данные о вероятности выхода из строя каждого из модулей. Это будут исходные вероятности, которые в дальнейшем в процессе работы при конкретных условиях могут корректироваться. Каждая из поломок (неисправностей) каждого модуля характеризуется определенными признаками. Эти признаки представлены в виде вопросов, на которые можно ответить либо «да», либо «нет». Алгоритм реализован в виде следующих этапов.

Этап 1. Ввод исходных данных (неисправности, количество неисправностей, характеристики неисправностей). Каждая неисправность характеризуется набором признаков неисправностей: характерные признаки (есть всегда), нехарактерные признаки (нет всегда), полухарактерные признаки (промежуточные признаки между характерными и нехарактерными, могут быть с некоторой вероятностью).

Например, при анализе работоспособности модуля «зрение», к характерным признакам относятся видимость (вопрос: четко ли виден объект наблюдения?), к нехарактерным - вопрос о звуке (вопрос: издает ли объект звук?), к полухарактерным - вопрос о движении (вопрос: движется ли объект?). Тогда информация может быть записана в виде последовательности:

$$(A, P_A, N1^1, P1_1^1, P1_2^1, N1^2, P1_1^2, P1_2^2, \ldots\ldots\ldots\ldots\ldots\ldots, N1^j, P1_1^j, P1_2^j,$$
$$N2^1, P2_1^1, P2_2^1, N2^2, P2_1^2, P2_2^2, \ldots\ldots\ldots\ldots\ldots\ldots N2^k, P2_1^k, P2_2^k,$$
$$N3^1, P3_1^1, P3_2^1, N3^2, P3_1^2, P3_2^2, \ldots\ldots\ldots\ldots\ldots\ldots N3^m, P3_1^m, P3_2^m),$$

где A – номер неисправности, P_A – вероятность неисправности с номером A; $N1^i$ - номера характерных признаков (вопросов) (j – количество характерных признаков (вопросов), $1 \le i \le j$), $P1_1^i$ - вероятность ответа «да» на i – ый вопрос, $P1_2^i$ - вероятность ответа «нет» на i – ый вопрос; $N2^i$ - номера нехарактерных признаков (вопросов) (k – количество нехарактерных признаков (вопросов) $1 \le i \le k$), $P2_1^i$ - вероятность ответа «да» на i – ый вопрос, $P2_2^i$ - вероятность ответа «нет» на i – ый вопрос; $N3^i$ - номера полухарактерных признаков (вопросов) (m – количество полухарактерных

признаков (вопросов) $1 \le i \le m$), $P3_1^i$ - вероятность ответа «да» на i – ый вопрос, $P3_2^i$ - вероятность ответа «нет» на i – ый вопрос, причем $P1_1^i+P1_2^i=1$, $P2_1^i+P2_2^i=1$, $P3_1^i+P3_2^i=1$ и сумма всех P_A по всем неисправностям А равна 1.

Количество вопросов характерных, нехарактерных и полухарактерных удовлетворяет неравенствам $j \ge 1$, $k \ge 1$, $m \ge 1$. Общее количество вопросов $V_{вопросов} = j+k+m$ и вопросы хранятся в виде пронумерованного списка.

Этап 2. Ввод вопроса. Выбирается вопрос из списка вопросов, на который ответу «да» соответствует неисправность с максимальной вероятностью.

Этап 3. Из списка неисправностей выделяется новый список неисправностей, удовлетворяющих условию: на заданный вопрос ответу "да" соответствует вероятность $P>P^*$, где $0<P^*<1$. Конкретное значение числа P^* зависит от решаемой задачи.

Этап 4. Выбор вопроса осуществляется следующим образом. Просматриваем все численные значения вероятности с ответом "да" на характерные, нехарактерные и полухарактернве вопросы и выбирается наибольшее значение вероятности. Если их оказалось больше 1, то выбираем любой. Максимальному значению вероятности соответствует некоторый вопрос, который и задается. На этот вопрос можно ответить "да" или "нет". Этот вопрос исключаем из общего списка вопросов.

Этап 5. Если на вопрос ответ "да", то просматриваются все значения вероятности с ответом "да" на характерные. нехарактерные и полухарактерные вопросы и выбирается наибольшее. Если их несколько, то выбирается любое. Этому выбору соответствует новый вопрос, который задается и исключается из списка вопросов. Из списка неисправностей убираются неисправности, в которых на этот вопрос (номер этого вопроса) вероятность ответа «да» $P<P^{**}$, где $0<P^{**}<1$. Конкретное значение числа P^{**} зависит от задачи. Если на вопрос ответ "нет", то просматриваем все значения вероятности с ответом "нет" на характерные, нехарактерные и полухарактерные вопросы и выбираем наименьшее. Если их больше 1, то выбираем любое. Этому выбору соответствует новый вопрос, который задается и исключается из списка. Из списка убираются неисправности, в которых на этот вопрос (номер этого вопроса) вероятность ответа «нет» $P>P^{***}$, где $0<P^{***}<1$. Конкретное значение числа P^{***} зависит от задачи.

Этап 6. Проверка количества оставшихся неисправностей. Если их больше 1, то осуществляется переход на этап 4. Иначе, эта неисправность является ответом.

Таким образом, список неисправностей постепенно сокращается и в итоге останется одна неисправность, которая является ответом. Можно составить ранжированный список неисправностей, по мере их исключения из общего списка неисправностей. Можно взять несколько неисправностей, которые были удалены в конце процедуры последними. Окончательное решение эксперта о неисправности принимается им самостоятельно, и вся ответственность лежит на нем.

Этап 7. Коррекция вероятностей. Эксперт загружает обучающую выборку. В качестве обучающей выборки можно использовать, например, список неисправностей за последний год, выявленных в процессе работы системы. На основании этих данных эксперт определяет вероятности ответа на тот или иной вопрос. Например, нарушение работы модуля «зрение» было 100 раз, нечеткость видимости объекта была во всех случаях, а подвижность объекта наблюдения была только в 40 случаях и т.д. При проведении новых наблюдений вероятности периодически пересчитываются и перезаписываются в таблицу, хранящуюся в памяти компьютера. Количество новых наблюдений, после которых вероятности пересчитываются, может быть любым, например, можно взять 100 или 1000 в зависимости от конкретной задачи. Коррекцию вероятностей можно записать следующим образом. Если до коррекции было *NN* наблюдений и для *A* - ой неисправности имели

$$(A, P_A, N1^1, P1_1^1, P1_2^1, N1^2, P1_1^2, P1_2^2, \ldots\ldots\ldots\ldots\ldots\ldots, N1^j, P1_1^j, P1_2^j,$$
$$N2^1, P2_1^1, P2_2^1, N2^2, P2_1^2, P2_2^2, \ldots\ldots\ldots\ldots\ldots\ldots N2^k, P2_1^k, P2_2^k,$$
$$N3^1, P3_1^1, P3_2^1, N3^2, P3_1^2, P3_2^2, \ldots\ldots\ldots\ldots\ldots\ldots N3^m, P3_1^m, P3_2^m),$$

а после провели еще MM наблюдений и с неисправностью А было А1 случаев, из которых:

– на вопрос с номером $N1^i$ ($1 \le i \le j$) ответ «да» был в $N1p^i$ случаях и «нет» – в $N1m^i$ случаях,
– на вопрос с номером $N2^i$ ($1 \le i \le k$) ответ «да» был в $N2p^i$ случаях и «нет» – в $N2m^i$ случаях,
– на вопрос с номером $N3^i$ ($1 \le i \le m$) ответ «да» был в $N3p^i$ случаях и «нет» – в $N3m^i$ случаях,

то после коррекции будем иметь

$$(A, P_A^N, N1^1, P1_1^{1N}, P1_2^{1N}, N1^2, P1_1^{2N}, P1_2^{2N}, \ldots\ldots\ldots\ldots, N1^j, P1_1^{jN}, P1_2^{jN},$$
$$N2^1, P2_1^{1N}, P2_2^{1N}, N2^2, P2_1^{2N}, P2_2^{2N}, \ldots\ldots\ldots\ldots N2^k, P2_1^{kN}, P2_2^{kN},$$
$$N3^1, P3_1^{1N}, P3_2^{1N}, N3^2, P3_1^{2N}, P3_2^{2N}, \ldots\ldots\ldots\ldots N3^m, P3_1^{mN}, P3_2^{mN}),$$

и новые значения вероятностей

$$P_A^N, P1_1^{1N}, P1_2^{1N}, P1_1^{2N}, P1_2^{2N}, \ldots\ldots\ldots\ldots, P1_1^{jN}, P1_2^{jN},$$
$$P2_1^{1N}, P2_2^{1N}, P2_1^{2N}, P2_2^{2N}, \ldots\ldots\ldots\ldots, P2_1^{kN}, P2_2^{kN},$$
$$P3_1^{1N}, P3_2^{1N}, P3_1^{2N}, P3_2^{2N}, \ldots\ldots\ldots\ldots, P3_1^{mN}, P3_2^{mN}$$

можно определить следующим образом:

$$P_A^N = (NN \cdot P_A + A1) / (NN + MM),$$
$$P1_1^{iN} = (NN \cdot P_A \cdot P1_1^i + N1p^i) / (NN \cdot P_A + A1),\ P1_2^{iN} = 1 - P1_1^{iN},\ 1 \le i \le j,$$

$$P2_1^{iN} = (NN \cdot P_A \cdot P2_1^{i} + N2p^{i}) / (NN \cdot P_A + A1),\ P2_2^{iN} = 1 - P2_1^{iN},\ 1 \le i \le k,$$
$$P3_1^{iN} = (NN \cdot P_A \cdot P3_1^{i} + N3p^{i}) / (NN \cdot P_A + A1),\ P3_2^{iN} = 1 - P3_1^{iN},\ 1 \le i \le m,$$

где NN+MM – общее число случаев после коррекции, NN . Pi - число случаев с неисправностью А до коррекции, (NN PA + A1) - число случаев с неисправностью А после коррекции.

Этап 9. Поддержка принятия решений в каждом классе осуществляется в подсистемах «9-1», …, «9-l», …, «9-n».

Этап 10. Сбор сгенерированных решений из всех классов осуществляется в подсистеме «10» и затем на их основе осуществляется генерация новой совокупности решений.

Этап 11. В подсистеме «11» осуществляется сравнение принятого решения с решениями, принятыми ранее на основе сравнения с информацией хранящейся в подсистеме «14».

Этап 12. В подсистеме «12» осуществляется выработка устойчивой реакции на многократно поступающую информацию и ее закрепление, путем сравнения с ранее полученной информацией и хранящейся в подсистеме «14».

Этап 13. В подсистеме «13» осуществляется поддержка принятия решений и генерируется совокупность решений.

Этап 14. Подсистема «14» включает в себя хранилище информации поступившей ранее. В подсистеме «14» на основе вновь записанной информации и путем сравнения с ранее записанной информацией генерируется новая информация.

Таким образом, построена система моделей и алгоритмов обработки слабо формализованной информации, поступающей от технических систем. Важными элементом этой системы являются модули, ответственные за сохранение конфиденциальности данных, в частности, оценивание достоверности полученной информации о нарушении конфиденциальности данных (модуль 5), оценивание безопасности полученной информации (модуль 6), оценивание вероятности, с которой можно доверять вновь полученной информации о нарушении конфиденциальности (модуль 8). Результат обработки информации в модулях 5, 6 и 8 оказывает существенное влияние на поддержку принятия решений и дальнейшую работу всей системы (модули 9, 12, 13)

СПИСОК ЛИТЕРАТУРЫ

1. Копыльцов А.А. Алгоритм коррекции связей между фрагментами слабо формализованной информации и генерация новой информации // Вестник Нижневартовского государственного университета. – 2014. - № 3. - С. 28-34.
2. Копыльцов А.А. Модель классификации информации и алгоритм ее предварительной обработки для статических и динамических объектов // Известия СПбГЭТУ “ЛЭТИ” (известия государственного электротехнического университета), серия “Информатика, управление и компьютерные технологии”. – 2013. – № 6. – С.134-139.
3. Копыльцов А.А., Копыльцов А.В. Алгоритм обработки слабо формализованной информации, поступающей от технических систем // Известия СПбГЭТУ “ЛЭТИ” (известия государственного электротехнического университета), серия “Информатика, управление и компьютерные технологии”. – 2012. – № 8. – С.30 – 36.
4. Копыльцов А.А., Копыльцов А.В. Обобщенный алгоритм обработки слабо формализованной информации и его применение // Вестник Нижневартовского государственного университета. – 2014. - № 35. - С. 35-44.
5. Копыльцов А.А., Копыльцов А.В.. Обработка слабо формализованной информации, поступающей от технических систем // Вестник Нижневартовского государственного гуманитарного университета. – 2013. – № 1. – С. 32-36.

УДК 004.056.53

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ВОЛОКОННО-ОПТИЧЕСКОГО КАНАЛА СВЯЗИ ОТ УГРОЗЫ ПЕРЕХВАТА ТРАФИКА

Кудрявцева Ксения Александровна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверский проспект, 49,
e-mail: kudriavtseva.ksyu@yandex.ru

Аннотация: в данной статье рассмотрены меры, с помощью которых можно предотвратить несанкционированное подключение к каналу ОВ связи для съема трафика, а так же способы криптографической защиты информации, необходимые для минимизации вероятности получения конфиденциальной информации злоумышленником.

Ключевые слова: *информационная безопасность, оптический сигнал, оптоволоконная линия связи, криптография, защищенность от угроз.*

PROTECTION ASSAY FIBER-OPTIC LINK FROM THE THREAT OF INTERCEPT TRAFFIC

Ksenia Kudriavtseva,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: kudriavtseva.ksyu@yandex.ru

Abstract: This article describes the steps you can use to prevent unauthorized connection to the communication channel OB for removal of traffic, as well as methods of cryptographic protection of information required to minimize the likelihood of confidential information by an attacker.

Keys words: *information security, optical signal, the optovolokonnaya line of communications, cryptography, protection from the threats.*

Введение. 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 [1].

С одной стороны, внедрение таких технологий создает иллюзию большей защищенности информации, что объясняется новизной используемых принципов, для которых еще не разработаны каналы утечки. С другой стороны, существует опасность появления каналов утечки еще не выявленных и не рассматриваемых ранее. Подобная проблема возникает с применением фотонных технологий в обработке, передаче и хранении информации, а именно с волоконно-оптической линией связи.

Оптический кабель – это кабель на базе оптических волокон. Волоконная оптика основывается на эффекте преломления при максимальном угле падения, когда имеет место полное отражение. Это явление происходит в том случае, когда луч света выходит из плотной среды и попадает в менее плотную среду под определенным углом.

Внутренняя жила кабеля ВОЛС имеет более высокий показатель преломления, чем оболочка и возникает эффект полного отражения. По этой причине луч света, проходя по внутренней жиле, не может выйти за ее пределы.

Оптические кабели позволяют достичь значительных преимуществ по сравнению с другими, привычными для нас медными и электрическими кабелями. Использование в качестве носителей информации коротких лазерных импульсов инфракрасного диапазона обеспечивает скорость передачи в несколько десятков гигабит в секунду, что превышает максимальные скорости радиосвязи и связи посредством электрических кабелей [2].

Оптическая кабельная инфраструктура объекта информатизации может включать не только локальную сеть, но и сети телефонной связи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по оптическим кабелям трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта независимо от вида сети. Трафик может подвергаться различным опасностям, таким как нарушение конфиденциальности, целостности и доступности.

ВОЛС может располагаться как в периметре предприятия, так и за его границами. Нужно понимать, как и где злоумышленник может подобраться к объекту информатизации. Для этого введем понятие контролируемой зоны.

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения [3].

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:

1. Физические средства защиты информации
2. Аппаратные средства защиты информации
3. Криптографическая защита информации

Рассмотрим каждый подробнее. Начнем с физических средств защиты информации.

Контроль доступа к оптическому кабелю – это метод контроля, в котором регистрируется физический доступ к оптическому кабелю возможных злоумышленников по их воздействию на оптический кабель, в виде вибраций, виброакустических и других полей создаваемых нарушителем [4].

1. 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.

Оптический тестер – это приборы, использующиеся для диагностики состояния оптоволоконных сетей и определения параметров, объединяет в себе измеритель оптической мощности, источник излучения.

Оптические тестеры позволяют проводить измерения, запоминать и передавать результаты замеров потерь канала, потерь на отражение на канале и длины канала.

Подробнее рассмотрим оптические рефлектометры, упоминаемые выше. Их работа в данной области обусловлена применением импульсной рефлектометрии. Это область измерительной техники, которая основывается на получении информации об измеряемой линии по анализу её реакции на зондирующее (возмущающее) воздействие, с возможностью определения расстояния до неоднородности в канале.

Метод импульсной рефлектометрии позволяет определить зону повреждения (в пределах погрешности измерения) и применить отдельные трассовые методы обнаружения только на небольших участках трассы, что позволяет существенно сократить время точного определения места дефекта.

С помощью оптического рефлектометра можно определить полную величину потерь в линии, местоположение обрыва волокон, участки линии с большими значениями потерь, коэффициенты отражения от соединительных разъемов и т.д. Используя для этого рефлектограмму.

Рефлектограмма – это графическое изображение результатов испытаний ОВ с использованием рефлектометра, в котором по горизонтальной оси отображается расстояние, а по вертикальной оси отображается уровень мощности оптического излучения, поступившего (возвращенного) на вход рефлектометра из испытываемого ОВ [5].

Рефлектограмма испытываемого ОВ должна отображаться на дисплее рефлектометра в следующем виде:

– по горизонтальной оси отображается расстояние;

– по вертикальной оси отображается уровень мощности оптического излучения, поступившего (возвращенного) на вход прибора из испытываемого ОВ.

Единицы измерения должны индицироваться:

– по горизонтальной оси (шкала расстояния) – в м или/и в км;

– по вертикальной оси (шкала затухания) – в дБ [5].

На рисунке 1 показан пример показаний, отраженных на дисплее оптического рефлектометра, с пояснениями данных показаний.

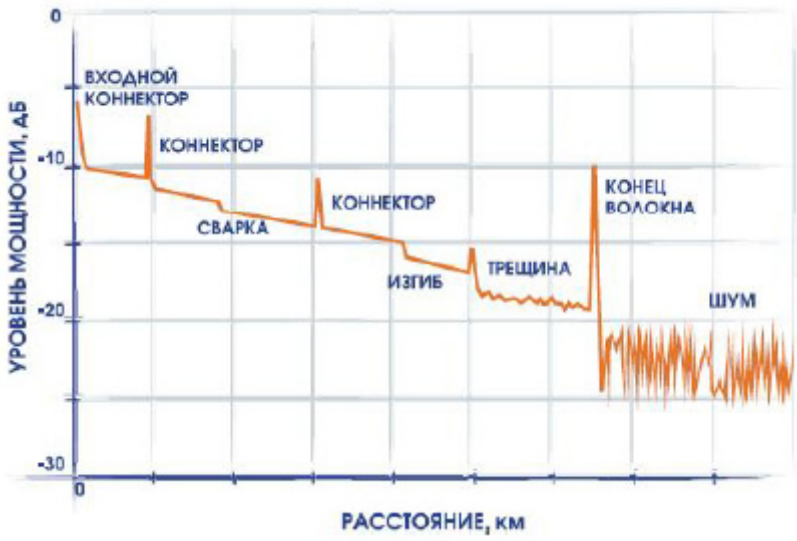


Рис. 1 Показания оптического рефлектометра.

С помощью оптического рефлектометра можно определить не только, где и в каких объемах потерян трафик, но и вид дефекта ОК, от чего и происходят данные потери.

Наряду с тестерами, рефлектометрами и мультиметрами используется другие виды наблюдения за ОК:

1). Мониторинг сигналов вблизи волокна.

Этот метод подразумевает производство оптоволокна с дополнительными волокнами, по которым передается специальный сигнал мониторинга. Использование такого метода увеличит стоимость кабеля, но любая попытка согнуть кабель вызывает потерю сигнала мониторинга, и вызывает срабатывание сигнала тревоги.

2) Электрические проводники.

Метод состоит в интегрировании электрических проводников в кабель, и если оболочка кабеля нарушена, то изменяется емкость между электрическими проводниками и это может использоваться для срабатывания тревоги.

3). Мониторинг мощности мод.

Этот метод применим к мультимодовому волокну, в котором затухание – это функция от моды, в которой распространяется свет. Подсоединение влияет на определенные моды, но при этом затрагивает и другие моды. Это приводит к перераспределению энергии от проводящих мод к непроводящим, что меняет соотношение энергии в ядре волокна и его оболочке. Изменение энергии в модах может быть обнаружено на принимающей стороне соответствующим измерением, что будет являться информацией для принятия решения – есть подключение к кабелю или нет.

4).Измерение оптически значимой мощности.

В волокне может осуществляться мониторинг уровня оптически значимой мощности. В том случае, если она отличается от установленного значения, срабатывает сигнал. Но это требует соответствующей кодировки сигнала так, чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации.

5).Методы с использованием пилотного тона.

Пилотные тоны проходят по волокну также как и коммуникационные данные. Они используются для обнаружения перерывов в передаче. Пилотные тоны могут использоваться для обнаружения атак, связанных с постановкой помех, но если несущие волновые частоты пилотных тонов не затрагиваются, то данный метод не является эффективным при обнаружении такого рода атак. О наличии подключения можно судить только по существенному уменьшению уровня сигнала пилотного тона [6].

Аппаратные средства защиты – средства защиты информации, реализованные на аппаратном уровне.

Рассмотрим метод случайного кодирования – кодовое зашумление. Способ рассмотрен в случае, когда злоумышленник подключен к ВОЛС посередине, как показано на рисунке 2.

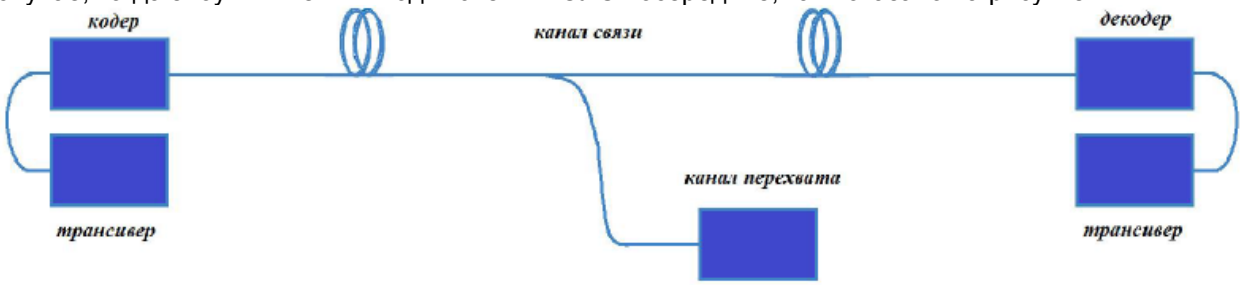


Рис. 2. Схема подключения злоумышленника

Это метод, заключающийся в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декодировании сигналов, получаемых из канала утечки информации.

Защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем штатный канал пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возрастало, обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь.

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.

Таким образом, квантовая криптография использует законы квантовой механики для гарантии безопасности распределения ключей. Это позволяет абонента сгенерировать случайный ключ, известный только им. Он может быть использован в шифровании или аутентификации.

В *заключении* **о**тметим, что каждый из этих методов по-отдельности не сможет полностью защитить информацию ограниченного доступа, от попадания ее за пределы КЗ, поэтому, чтобы минимизировать такую вероятность, нужно применять комплекс указанных мер, а так же проводить работу с персоналом.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО «Издательство Полигон», 2000. – 856 с.
2. Никоноров Н. В., Сидоров А. И, учебное пособие «Материалы и технологии волоконной оптики» // СПб, Редакционной-издательский отдел СПб ГУИТМО -2009 г., с. 22
3. Обеспечение информационной безопасности в организации// ГОСТ Р 53114-2008, Москва – 2009, с.6
4. Гришачев В. В.,Информационная безопасность волоконно-оптических технологий// учебно-методический курс – 3 раздел, Защита РИ в ВОК
5. M.Z IQBAL, H FATHALLAH, N BELHADJ. 2011. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies - 2011
6. Кудрявцева К. А., Сценарии подключения к оптоволоконным кабелям и защита от незаконного перехвата информации в каналах ОВ связи// ФГБОУ ВПО «Государственный университет морского и речного флота имени адмирала С.О. Макарова» - 2014

УДК 681.3

ВОПРОСЫ И РЕШЕНИЯ СОВРЕМЕННОЙ КРИПТОГРАФИИ ДЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Молдовян Александр Андреевич, Молдовян Николай Андреевич, Касаткин Виктор Викторович,
Санкт-Петербургский институт информатики и автоматизации РАН «СПИИРАН»,
Россия, Санкт-Петербург, В.О., ул. 14-линия, д. 39,
e-mail: maa1305@yandex.ru

Аннотация: Обсуждаются вопросы расширения функциональности стандартов электронной цифровой подписи, формального доказательства стойкости алгоритмов, основанных на сложности задачи дискретного логарифмирования. Рассматривается повышение уровня безопасности криптосхем, повышение стойкости при шифровании сообщений с использованием ключей малого размера. Предложен подход к построению алгоритмов и протоколов отрицаемого шифрования, основанный на реализации процедуры криптографического преобразования вычислительно неотличимого от вероятностного шифрования.

Ключевые слова: *стандарты электронной цифровой подписи; стойкость алгоритмов электронной цифровой подписи; криптосистемы с открытым ключом; отрицаемое шифрование*

QUESTIONS AND SOLUTIONS OF MODERN CRYPTOGRAPHY FOR COMPUTER SYSTEMS

Moldovyan Alexander Andreevich, MoldovyanNikolayAndreevich, Kasatkin Victor Victorovich,
The St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
Russia, Saint-Petersburg, 14 line, the house 39,
e-mail: maa1305@yandex.ru

Abstract:Discussed the issues of expanding the functionality of the electronic digital signature standards, formal proofs resilienceof cryptographic algorithms based on the complexity of the problem of discrete logarithm. Discusses the improvement of safety of cryptographic schemes to improve the resilience when encrypting messages using keys of small size. The approach to constructing algorithms and protocols of *deniable* encryption, based on the implementation of the cryptographic transformation procedure is computational indistinguishable from a probabilistic encryption.

Keywords:*standards of a digital signature; firmness of algorithms of a digital signature, cryptosystems with an public-key; deniable encryption*

Введение

Криптографические алгоритмы и протоколы широко применяются для обеспечения информационной безопасности современных информационно-телекоммуникационных систем. При этом некоторые типы криптосистем лежат в основе новых информационных технологий, например, тех технологий, которые с необходимостью требуют решения задач аутентификации источника сообщений, придания юридической силы электронным сообщениям, обеспечения анонимности пользователей. Современная криптография является развитой ветвью современной прикладной математики и прикладной технической дисциплиной. Она предлагает широкий арсенал средств для решения разнообразных задач обеспечения информационной безопасности, однако практическая информатика выдвигает новые актуальные вопросы, стимулируя проведение новых научно-технических исследований и получение новых результатов.

В предлагаемой работе рассматриваются некоторые сравнительно новые вопросы криптографии и полученные результаты, связанные с их решением. Рассматриваются вопросы расширения функциональности стандартов электронной цифровой подписи (ЭЦП), формальное доказательство стойкости алгоритмов ЭЦП, основанных на сложности задачи дискретного логарифмирования (ЗДЛ), повышение уровня безопасности криптосхем, повышение стойкости при шифровании сообщений с использованием ключей малого размера, обеспечение защищенности секретной информации при так называемых «вынуждающих» атаках, в модели которых предполагается, что атакующему предоставляется ключ шифрования.

1. Расширение функциональности стандартов электронной цифровой подписи

Вопрос расширения функциональности официальных стандартов ЭЦП связан с тем, что большинство стандартов специфицируют схему индивидуальной цифровой подписи, тогда как практикой востребованы протоколы ЭЦП других типов, например, коллективной, групповой и слепой подписи. Принятие новых стандартов представляет собой долговременный и ресурсоемкий процесс. Взамен принятия самостоятельных стандартов на все востребованные типы протоколов ЭЦП, в работах [1–4] рассматривается подход, состоящий в использовании стандартизированной схемы индивидуальной ЭЦП для построения на ее базе протоколов следующих типов: 1) коллективной, 2) слепой и 3) слепой коллективной подписи. В данном подходе предполагается разработка таких протоколов последнего типа, для которых может быть дано редукционное доказательство стойкости (если протокол не является стойким, то не является стойкой и базовая схема, на основе которой построен протокол), причем для их практического внедрения не требуется внесение каких-либо изменений в существующую инфраструктуру открытых ключей. Было показано, что данный подход применим к стандартам ГОСТ Р.34.10–94, ГОСТ Р.34.10–2001, ГОСТ Р.34.10–2012, стандартам Беларуси СТБ 1176.2–99, Украины ДСТУ 4145–2002 и Германии ECGDSA.

Представляет интерес также и реализации протокола групповой подписи с маскированием открытых ключей подписантов, предложенного в работе [5], на основе указанных стандартов, однако это вопрос не отражен в известных публикациях.

2. Формальное доказательство стойкости стандартов электронной цифровой подписи

Формальное доказательство стойкости криптосистем с открытым ключом обеспечивает наиболее полное признание безопасности их использования. В случае схем ЭЦП, основанных на вычислительной трудности ЗДЛ, наиболее известный способ формального доказательства стойкости, предложенный в работе [6], применим к криптосхемам, в которых в процедуре генерации подписи сначала формируется параметр рандомизации (называемый также фиксатором), а затем вычисляется первый элемент ЭЦП в виде значения хэш-функции, которое вычисляется от сообщения с присоединенным к нему фиксатором. К таким схемам ЭЦП относится протокол ЭЦП Шнорра. Однако для наиболее известных стандартов такое доказательство неприменимо.

Другим подходом к формальному доказательству стойкости схем ЭЦП, основанных на ЗДЛ, является подход, предложенный в работе [7] и состоящий в выводе рассматриваемой схемы из протокола с нулевым разглашением, для которого формально доказывается, что сложность подделки правильного ответа на случайный запрос проверяющего имеет один порядок со сложностью ЗДЛ, положенной в основу протокола. Последний подход требует построения новых трехпроходных протоколов с нулевым разглашением с отрытым ключом, имеющим такой же вид, как и открытый ключ, используемый в схеме ЭЦП. Для решения этой задачи предлагается расширение типов протоколов с нулевым разглашением, основанное на толковании термина «нулевое разглашение», опирающегося на статистическую эквивалентность набором случайных параметров, генерируемых в ходе протокола, выполняемого с участием подлинного доказывающего, и наборов случайных параметров, генерируемых в ходе имитации процедуры аутентификации, выполняемой потенциальным злоумышленником. При использовании такого толкования физического смысла протоколов с нулевым разглашением становится возможным построение значительно более разнообразных протоколов рассматриваемого типа, в том числе и протоколов, которые могут быть преобразованы в схемы ЭЦП, задаваемые стандартами ГОСТ Р.34.10–94, ГОСТ Р.34.10–2001, ГОСТ Р.34.10–2012, СТБ 1176.2–99, ДСТУ 4145–2002, DSA, ECDSA и ECGDSA[9]. При этом для таких

протоколов с нулевым разглашением может быть дано формальное редукционное доказательство стойкости к подделке ответа на случайный запрос, причем доказательство опирается на стандартное предположение о стойкости используемой хэш-функции (такое же предположение лежит в основе общепризнанного способа формального доказательства стойкости схемы ЭЦП Шнорра, рассмотренного подробно в работах [6,9]). Поскольку в схеме ЭЦП построенной путем ее вывода из протокола с нулевым разглашением (т.е. путем преобразования последнего в схему ЭЦП) значение одного из элементов подписи фактически является ответом на случайный запрос, вычисляемый в зависимости от фиксатора и значения документа. Подделка подписи означает подделку правильного ответа в протоколе с нулевым разглашением, т.е. вычислительная сложность подделки подписи имеет один порядок со сложностью ЗДЛ, использованной для построения схемы ЭЦП.

3. Повышение безопасности криптосистем с открытым ключом

Для практического использования криптографических алгоритмов и протоколов (криптсхем) важны различные аспекты их реализации: стойкость, вычислительная сложность используемых процедур, аппаратная и программная реализация и др. При этом улучшение параметров криптосхем путем их модифицирования или построения новых алгоритмов и протоколов имеет смысл только в случае, когда это выполняется в рамках выполнения требования обеспечения заданного уровня стойкости. Понятие стойкости характеризует важнейшее свойство криптографических схем выдерживать всевозможные атаки и измеряется количеством определенных операций, которые нужно выполнить для случая применения наиболее эффективной известной атаки, чтобы взломать криптосхему. Принципиальным моментом для оценки стойкости является вопрос о лучшем известном алгоритмевзлома криптосхемы. Если для криптосхемы удается доказать формально ее стойкость, то этот вопрос переносится на используемую для построения криптосхемы вычислительно трудную задачу. Обычно для построения криптосхемв качестве базовых трудных задач используются давно известные и хорошо изученные вычислительно трудные задачи, для решения которых маловероятно появление прорывных решений (имеющих полиномиальную сложность), что означало бы взлом целого класса криптосхем, т.е. всех тех криптосхем, в основу которых была положена данная задача. Принципиальной проблемой оценки стойкости криптосхем является то, что трудно доказать, что не существуют или хотя бы в ближайшем будущем не будут найдены прорывные решения базовой трудной задачи, что дало бы твердое обоснование оценки стойкости криптосхемы как вычислительной сложности лучшего из известных в настоящее время алгоритмов указанной задачи.

Когда говорят о том, что криптосхема является стойкой в смысле безопасности ее использования для решения задач информационной безопасности, то явно полагают, что значение стойкости превосходит некоторое заданное достаточно большое значение, например, 2^{80} (80-битовая стойкость), 2^{128} (128-битовая стойкость) или 2^{192} операций (192-битовая стойкость). В тоже время неявно предполагается, что вероятность появления в обозримом будущем прорывных решений базовой трудной задачи (для доказуемо стойких двухключевыхкриптосхем) или появления прорывных атак (в общем случае) является пренебрежимо малой. Последнее положение также является принципиально важным, когда говорится о безопасности использования криптосхем для решения тех или иных задач практики. Понятие стойкости отражает только одну из двух сторон понятия безопасности криптосхем. Второй стороной является вероятность того, что в обозримом будущем не будут получены прорывные результаты по разработке алгоритмов решения используемых трудных задач.Количественная оценка безопасности должна включать количественные оценки стойкости и указанной вероятности, например, количественную меру безопасности можно задать как отношение стойкости к вероятности. Такая формула явно показывает, что повышение безопасности, обеспечиваемого криптосхемами, может быть достигнуто как увеличением размеров параметров криптосхемы, приводящим к росту значения стойкости, так и уменьшением значения указанной вероятности.

Эта трактовка понятия безопасности лежит в основе одного из направлений исследований в криптографии, связанном с построением криптосхем, взлом которых требует одновременного решения двух независимых трудных вычислительных задач. При построении таких криптосхем полагается, что вычислительная сложность каждой из используемых задач имеет значение, равное или превосходящее заданный уровень стойкости, а достижение повышения значения безопасности достигается за счет перемножения малых вероятностей, относящихся к событиям появления прорывных решений двух используемых трудных задач. В этом направлении наиболее часто использовано комбинировании задачи факторизации (ЗФ) целых чисел специального вида и ЗДЛ по простому модулю. Первоначально были разработаны протоколы ЭЦП данного типа [10–13]. Последние результаты этого направления исследований относятся к разработке общего подхода к построению криптосхем на основе трудности ЗФ и ЗДЛ по простому модулю [14,15]. Общий подход позволяет разработать алгоритмы и протоколы открытого согласования ключа, открытого шифрования, коммутативного шифрования, ЭЦП и др. Суть подхода состоит в использовании ЗДЛ по трудно разложимому модулю и основан на том, что субъэкспоненциальное решение последней задачи требует решения ЗФ составного модуля и решения ЗДЛ по модулю, равному каждому из

простых делителей модуля. При этом для случая реализации протоколов ЭЦП достигается повышение производительности и уменьшение размера подписи при заданном уровне стойкости.

4. Новый подход к построению алгоритмов и протоколов отрицаемого шифрования

Понятие отрицаемого шифрования (ОШ), впервые введенного в работе [16], связывается с задачей обеспечения стойкости шифрования в условиях возможности осуществления так называемых атак с принуждением. Данные виды атак подразумевают наличие у атакующего ресурсов воздействия на отправителя и/или получателя сообщений, которые вынуждают отправителя и/или получателя раскрыть параметры процесса зашифрования (принуждающая атака на отправителя сообщения) или расшифрования (принуждающая атака на получателя сообщения), например, ключ шифрования и случайные значения, использованные в процессе шифрования. Если предполагается, что атакующий может потребовать предоставления ему как параметров зашифрования, так и параметров расшифрования, то имеет место двухсторонняя принуждающая атака. Стойкость к таким атакам обеспечивается алгоритмами и протоколами ОШ тем, что выходной шифртекст (криптограмма) может быть получен из различных осмысленных исходных сообщений, и/или из криптограммы могут быть получены различные расшифрованные осмысленные тексты. Атакующему передаются параметры шифрования, которые связывают криптограмму с некоторым фиктивным осмысленным текстом. Атакующий проверяет то, что использование предоставленных ему параметров шифрования действительно приводит к преобразованию фиктивного сообщения в заданную криптограмму и/или к расшифрованию последней в фиктивное сообщение. Если результат проверки является положительным и атакующий не может доказать неполноту раскрытого текста, то алгоритм (протокол) ОШ считается стойким.

В известной литературе основное внимание исследователей посвящено способам ОШ, относящихся к криптосхемам с открытым ключом. Такие способы основаны на использовании алгоритмов открытого шифрования или на использовании протоколов открытого распределения ключей [17-19]. При этом предполагается, что отправитель и получатель не владеют заранее согласованной секретной информацией (разделяемого секретного ключа), а восстановление фиктивного/настоящего сообщения зависит от применяемых случайных значений.

Интерес к алгоритмам и протоколам ОШ связан с перспективами их применения в защищенных распределенных вычислениях и системах тайного электронного голосования [20,21]. Одно из ограничений практического использования процедур ОШ состоит в их низкой производительности, особенно характерной для криптосхем с открытым ключом. Поиск новых алгоритмов и протоколов ОШ привел к разработке более производительных способов ОШ [22,23], однако практика требует дальнейшего повышения скорости работы криптоалгоритмов, особенно в случаях применения способов ОШ как специального механизма защиты информации в комплексных средствах компьютерной безопасности, основанного на обманных ловушках [24].

В отличие от схем ОШ на основе асимметричных алгоритмов шифрования, ОШ, основанное на схемах с разделяемым ключом, подразумевает наличие общего секрета (общего секретного ключа), позволяющего восставить настоящее сообщение, как у отправителя, так и у получателя. В работах решена задача построения производительных алгоритмов отрицаемого шифрования с разделяемым ключом при одновременном обеспечении высокой стойкости к двухсторонней атаке. При этом отрицаемость шифрования обеспечивается вычислительной неотличимостью ОШ от вероятностного шифрования. Использование последнего принципа перспективно также и для построения алгоритмов ОШ с открытым ключом, при вынуждающей атаке которых предполагается получение атакующим значения личного секретного ключа.

Заключение

Возможность использования процедур формирования и проверки ЭЦП, специфицируемых рядом официальных стандартов ЭЦП в протоколах слепой и коллективной подписи показывает, что последние могут найти более широкое применение по сравнению с их первоначальным предназначением. Это показывает, что используемая в них схема ЭЦП предпочтительнее, чем схема ЭЦП американских стандартов DSA и ECDSA, для которых указанное расширение функциональности не может быть осуществлено.

Предложенный подход к формальному доказательству стойкости стандартов ЭЦП является существенным вкладом в обоснование их стойкости и ставит их в один ряд с доказуемо стойкими алгоритмами ЭЦП.

Рассмотренная концепция реализации процедуры ОШ как процедуры криптографического преобразования вычислительно неотличимого от вероятностного шифрования представляет интерес для построения алгоритмов ОШ по открытому ключу, что, видимо, позволит решить проблему обеспечения высокой скорости таких алгоритмов и расширить области их потенциального применения.

Указанные результаты использованы при подготовкеучебных материалов программ повышения квалификации специалистов, разработанных вСанкт-Петербургском институте информатики и автоматизации Российской академии наук.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Н.А., Дерова Е.С., Молдовян Д.Н. Расширение функциональности стандартов электронной цифровой подписи России и Беларуси // Вопросы защиты информации. 2011. №2.С.8–14.
2. Молдовян Н.А., Дерова Е.С., Молдовян Д.Н. Протоколы слепой и коллективной подписи на основе стандарта ЭЦП ДСТУ 4145-2002 // Вопросы защиты информации. 2011. №2. С.14–18.
3. Moldovyan N.A. Blind Signature Protocols from Digital Signature Standards // Int. Journal of Network Security. 2011. Vol. 13, No 1. P. 22–30.
4. Кочубинский А.И., Молдовян Н.А., Фаль А.М. Слепые мультиподписи на основе стандартов ДСТУ 4145-2002 и ГОСТ Р 34.10-2001// ДоповідіНаціональноїакадемії наук України. 2012. №3. С.38–43.
5. Молдовян А.А., Молдовян Н.А., Латышев Д.М., Головачев Д.А.Протокол групповой цифровой подписи на основе маскирования открытых ключей// Вопросы защиты информации. 2011. №3. С.2–6.
6. D. Pointcheval and J. Stern. Security Arguments for Digital Signatures and Blind Signatures. J. Cryptology, 2000, vol. 13, p.361–396.
7. Молдовян А.А., Молдовян Д.Н., Васильев И.Н., Головачев Д.А. Протоколы с нулевым разглашением секрета и обоснование безопасности схем цифровой подписи // Вопросы защиты информации. 2011. №4.С.6–11.
8. International Standard ISO/IEC 14888-3:2006(E). Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms.
9. Koblitz N. and Menezes A.J. Another Look at “Provable Security // J. Cryptology. 2007. V. 20. P. 3–38.
10. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. №1. С.22–26.
11. Кишмар Р.В., Молдовяну П.А., Новикова Е.С., Сухов Д.К. «Протоколы слепой подписи на основе сложности одновременного решения двух трудных задач // Известия СПбГЭТУ «ЛЭТИ». 2011. №4. С.44–48.
12. Дернова Е.С., Молдовян Н.А. Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Безопасность информационных технологий. 2008 №2. С.79–85.
13. Minh N.H., Binh D.V., Giang N.T., Moldovyan N.A. Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems // Applied Mathematical Sciences. 2012. V. 6. No 139. P. 6903 – 6910.
14. Moldovyan N.A., Shcherbakov V.A. New Signature Scheme Based on Difficulty of finding roots // Quasigroups and Related Systems. 2012. Vol. 20. P. 261–266.
15. Демьянчук А.А., Молдовян Д.Н., Новикова Е.С., Гурьянов Д.Ю. Подход к построению криптосхем на основе нескольких вычислительно трудных задач // Информационно-управляющие системы. №2. 2013. С.60–66.
16. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption // Advances in Cryptology – CRYPTO 1997. Procedings. P. 90–104.
17. Ibrahim M.H. A Method for Obtaining Deniable Public-Key Encryption // International Journal of Network security. 2009. Vol. 8, No.1, P. 1–9.
18. Ibrahim M.H. Receiver-Deniable Public-Key Encryption // International Journal of Network security. 2009. Vol. 8, No.2. P. 159–165.
19. Klonowski M., Kubiak P., Kutyiowsk M. Practical Deniable Encryption // SOFSEM 2008: Theory and Practice of Computer Science,34th Conference on Current Trends in Theory and Practice of Computer Science, NovэSmokovec, Slovakia, January 19–25. 2008. P. 599–609.
20. Canetti R., Gennaro R. Incoercible multiparty computation // Proceedings of the 37th Annual Symposium on Foundations of Computer Science (October 14 – 16, 1996). FOCS. IEEE Computer Society, Washington, DC, 504.
21. Bo Meng. A Secure Internet Voting Protocol Based on Noninteractive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext // Journal of Networks. 2009. Vol. 4. No.5. P. 370–377.
22. Bresson E., Catalano D., Pointcheval D. A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications // Proceedings of the Aciacrypt 2003 conference.LNCS 2894, Berlin: Springer-Verlag, 2003. P. 37–54.
23. Bo Meng, Jiang Qing Wang. A Receiver Deniable Encryption Scheme // Proceedings of the 2009 International Symposium on Information Processing (ISIP’09) Huangshan, P. R. China, August 21–23, 2009. P. 254–257
24. Березин А.Н., Биричевский А.Р., Молдовян Н.А., Рыжков А.В. Способ отрицаемого шифрования // Вопросы защиты информации. 2013. №2. С.18–21.

УДК 681.3

ОТРИЦАЕМОЕ ШИФРОВАНИЕ НА ОСНОВЕ СТАНДАРТНОЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Молдовян Александр Андреевич[1], Березин Андрей Николаевич[2], Михтеев Михаил Сергеевич[2],
[1] Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, В.О., ул. 14-линия, д. 39,
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
им. В.И. Ульянова (Ленина)
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mail: maa1305@yandex.ru

Аннотация: В статье предлагается новый протокол отрицаемого шифрования на основе стандартной инфраструктуры открытых ключей. Протокол основан на вычислительной неотличимости шифртекста порождаемого алгоритмом вероятностного шифрования от шифртекста порождаемого алгоритмом отрицаемого шифрования. Предложенный протокол не использует общие секретные ключи, является стойким к двусторонним принуждающим атакам и активным принуждающим атакам, когда злоумышленник выдаёт себя за легального участника протокола.

Ключевые слова: *отрицаемое шифрование; шифрование с открытым ключом; вероятностное шифрование; аутентификация, задача дискретного логарифмирования*

BI-DENIABLE PUBLIC-KEY ENCRYPTION BASED ON STANDARD PKI

Moldovyan Alexander Andreevich[1], Berezin Andrey Nikolaevich[2], Mihteev Mikhail Sergeevich[2],
[1] The St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
Russia, St. Petersburg, 14 line, the house 39,
[2] The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str. 5,
e-mail: maa1305@yandex.ru

Abstract: there is discussed a new protocol for public-key deniable encryption that is free from using any shared key. The method is based on using the public-key encryption algorithm producing the cryptogram that is computationally indistinguishable from the ciphertext produced by some probabilistic public-key encryption algorithm. The proposed algorithm provides deniability when coercive adversary attacks both the party sending message and the party receiving message.

Keywords: *deniable encryption; public-key encryption; probabilistic ciphering; entity authentication; discrete logarithm problem*

Введение. Понятие отрицаемого шифрования (ОШ) было предложено в 1997 году [1]. Оно обозначает новый тип криптографических примитивов для использования в протоколах стойких к так называемым атакам с принуждением. Существуют различные варианты протоколов ОШ, которые стойкие к атакам на получателя, отправителя или на обоих держателей шифртекста. В модели принуждающих атак рассматривается нарушитель, который имеет некоторый ресурс воздействия на всех участников протокола, который заставляет их открыть всё секретную информацию связанную с криптограммой, т.е. открыть свои личные секретные ключи, используемые при шифровании, исходное сообщение соответствующее шифртексту и алгоритм шифрования. Предложенный [1] алгоритм ОШ показал принципиальную возможность построения протоколов, способных противостоять принуждающим атакам, однако он не подходит для практического использования из-за низкой скорости работы и итеративных процедур.

Область применения алгоритмов ОШ включает в себя защиту от скупки голосов при электронном голосовании [2] и безопасными многосторонними вычислениями [3]. Основным свойством алгоритмов ОШ является расшифрование шифртекста в разные открытые тексты с использованием различных ключей. Эта возможность появляется благодаря использованию некоторого случайного параметра r в процессе шифрования. В случае принуждающей атаки атакующему со стороны отправителя шифртекста c предоставляется подложное сообщение m и демонстрируется алгоритм вероятностного шифрования сообщения, который порождает данный шифртекст при использовании некоторого случайного параметра $r' \neq r$ и открытого ключа получателя в процессе шифрования. Со стороны получателя предоставляется полученный шифртекст и демонстрируется алгоритм расшифрования, который получает исходное сообщение m, получаемое с использованием личного секретного ключа получателя из шифртекста c.

В зарубежной литературе предложены алгоритмы ОШ с использованием открытых ключей [4], [5], [6], которые отличаются следующими свойствами: 1) использованием итеративного механизма пересылки сообщения (пошаговые схемы); 2) использованием общего секретного ключа (схемы с разделяемым секретом); 3) выбором подложного сообщения перед выполнение алгоритма ОШ (схемы с заранее сформированным подложным сообщением). Для практического применения интересны схемы, которые не используют пошаговые механизмы и общего секрета. Однако данные схемы используют оба секретных ключа и отправителя и получателя. Кроме этого такие схемы не обеспечивают стойкость к двусторонним принуждающим атакам.

В данной работе предлагается новый ассиметричный алгоритм ОШ с заранее сформированным подложным сообщением, который в отличие от существующих алгоритмов использует только открытый ключ получателя в процессе шифрования и обладает стойкостью к двусторонним принуждающим атакам. Предлагаемый алгоритм не использует разделяемых секретов, использует существующую инфраструктуру открытых ключей, и состоит из двух интерактивных шагов: на первом шаге выполняется аутентификация отправителя, на втором – ОШ.

Модель принуждающих атак и критерии построения алгоритмов ОШ. После того как шифртекст был послан отправителем, атакующий может заставить предоставить следующее:

1) открытое сообщение соответствующее шифртексту;
2) личный секретный ключ отправителя;
3) личный секретный ключ получателя;
4) алгоритм расшифрования, выходной открытый текст которого зависит от каждого бита входного.

Также активный атакующий может послать шифртекст, содержащий секретное и подложное сообщения, а затем принудить получателя расшифровать шифртекст. Если получатель раскроет фиктивное сообщение, то получатель будет уличен в обмане, что означает успешность атаки.

Для обеспечения стойкости к двусторонним атакам и нападениям активного нарушителя были предложены следующие требования к построению алгоритмов ОШ с открытым ключом:

1) алгоритм должен содержать два интерактивных шага и выполнять аутентификацию отправителя;

2) в процессе шифрования должны использоваться только открытый ключ получателя и случайные значения (т.е. без использования открытого ключа отправителя и секретных разделяемы ключей).

3) алгоритм ОШ должен ассоциироваться с алгоритмом вероятностного шифрования в том смысле, что криптограмма, сформированная в результате ОШ, в принципе могла бы быть порождена алгоритмом вероятностного шифрования фиктивного сообщения по фиктивному ключу.

Предлагаемый протокол. Пусть отправитель хочет отправить секретное сообщение t получателю. Тогда необходимо выполнить следующие шаги.

1) Получатель генерирует случайное значение r и подписывает это значение своей подписью $Sign_B(r)$, затем отправляет его отправителю.

2) Отправитель проверяет подпись $Sign_B(r)$ получателя. Если подпись верна, то отправитель генерирует подставное сообщение m, и шифрует его по открытому ключу получателя с использованием случайного значения r одновременно с секретным сообщением t, которое он хочет передать, в шифртекст c. Причём шифртекст c может быть получен с помощью некоторого алгоритма вероятностного шифрования подложного сообщения m с использованием открытого ключа получателя и случайного значения $r' \neq r$. Затем отправитель подписывает шифртекст c своей подписью $Sign_A(c)$ и посылает подпись и шифртекст получателю.

После получения шифртекста c получатель проверяет подпись $Sign_A(c)$. Если подпись верна, он расшифровывает шифртекст, содержащий сообщение, если подпись не верна – отвергает.

Для практического применения протокола используется стандартная инфраструктура открытых ключей, в которой они генерируются по аналогии с открытыми ключами в протоколе электронной цифровой подписи Эль-Гамаля [7,9] $y = a^x \bmod p$, где p это 2048 битное простое число такое, что $p-1$ содержит 256 битный простой делитель q, a – примитивный элемент по модулю p, x – секретный ключ. Так же предлагается использовать в алгоритме шифрования (аналог алгоритма открытого шифрования Эль-Гамаля) открытый ключ получателя $y_B = a^{x_B} \bmod p$, где x_B – секретный ключ получателя, т.е. процедура ОШ использует стандартные ключи, которые используются для генерации электронных цифровых подписей (см. 8, 9).

Значение r генерируется по формуле $r = a^k \bmod p$, где k – случайно генерируемое значение $q < k < p-1$. Это позволяет отправителю и получателю сформировать пару одинаковых значений Z и Q, которые невозможно вычислить, зная параметры и значения, передаваемые по каналу связи. ОШ выполняется таким образом, что существует ассоциированный алгоритм вероятностного шифрования, порождающий такую же криптограмму.

Ассоциированный алгоритм вероятностного шифрования.

1) Сгенерировать пару случайных значений $r' < p$, $w < p-1$ и вычислить $W = a^w \bmod p$.

2) Вычислить $Z = y_B{}^w \bmod p$.

3) Решить систему сравнений с неизвестными c_1 и c_2:

$$\begin{cases} Zc_1 + Z^2 c_2 = m \bmod p \\ c_1 = r' c_2 \bmod p \end{cases}$$

4) Послать шифртекст (W, c_1, c_2) получателю.

Получатель расшифровывает шифртекст (W, c_1, c_2), используя следующий алгоритм.

1) Вычислить значение $Z = W^{x_B} \bmod p$, где x_B – личный секретный ключ получателя.

2) Вычислить значение подложного сообщения $m = Zc_1 + Z^2 c_2 \bmod p$.

Алгоритм ОШ для секретного сообщения при $t < p$.

1) Получатель генерирует случайное значение $k < p-1$ и вычисляет значение $r = a^k \bmod p$. Затем подписывает значение $Sign_B(\mathrm{r})$ и посылает отправителю подпись $Sign_B(\mathrm{r})$ и значение r.

2) Отправитель проверяет подпись. Если подпись не верна, то сеанс связи прекращается. В противном случае, отправитель генерирует подложное сообщение $m < p$, случайное значение $w < p-1$ и вычисляет значение $W = a^w \bmod p$. Затем вычисляет значения $Z = y_B{}^w \bmod p$ и $K = r^w \bmod p$, где y_B – открытый ключ получателя, а r – полученное значение, и решает систему сравнений с неизвестными c_1 и c_2:

$$\begin{cases} Zc_1 + Z^2 c_2 = m \bmod p \\ Kc_1 + K^2 c_2 = t \bmod p \end{cases}.$$

Затем отправитель подписывает значение $c = (W, c_1, c_2)$ и отправляет его вместе с подписью $Sign_A(\mathrm{c})$ получателю. Получатель проверяет подпись $Sign_A(\mathrm{c})$, если она не верна – прекращает сессию.

Для расшифровки секретного сообщения t, получатель использует следующий алгоритм:

1) Вычислить значение $K = W^k \bmod p$ (где k – значение, сгенерированное получателем в начале сессии).

2) Вычислить значение секретного сообщения $t = Kc_2 + K^2 c_2 \bmod p$.

В случае принуждающей атаки получатель использует следующий алгоритм:

1) Вычислить значение $Z = W^{x_B} \bmod p$ (где x_B – личный секретный ключ получателя).

2) Вычислить значение секретного сообщения $m = Zc_2 + Z^2 c_2 \bmod p$.

Легко видеть, что алгоритмы расшифровки отличаются только используемыми в них значениями, для расшифровки из криптограммы подложного сообщения используется личный секретный ключ получателя x_B, а для расшифровки секретного сообщения используется случайное значение k, сгенерированное получателем в начале сессии.

Обсуждение. Предлагаемый протокол обеспечивает выполнение аутентификации отправителя, не использует открытый ключ отправителя в процессе шифрования, случайное значение r', используемое в ассоциированном алгоритме вероятностного шифрования, может быть легко вычислено $r' = c_1 / c_2 \bmod p$, которое приводит к генерации криптограммы $c = (W, c_1, c_2)$, отправленной получателю. Это позволяет защититься от двусторонней принуждающей атаки. В случае такой атаки отправитель открывает подложное сообщение m, которое может быть зашифровано с использованием открытого ключа получателя y_B и случайного значения r' в криптограмму c. А получатель открывает свой личный секретный ключ x_B, при использовании которого из криптограммы c расшифровывается подложное сообщение m, причём каждый бит сообщения зависит от каждого бита криптограммы. У атакующего не будет доводов полагать, что в криптограмме, помимо сообщения m, есть какое-либо другое сообщение.

Аутентификация, выполняемая на первом шаге, позволяет противостоять активным атакам, когда нарушитель пытается выдать себя за отправителя или получателя. Пусть атакующий выдаёт себя за получателя, и пытается разоблачить отправителя. Для этого он будет использовать случайное значение r, которое уже было подписано ранее настоящим получателем. Так как отправитель использует случайное значение w, которое влияет на значения K, Z для каждой сессии, то такая атака не будет успешной. А реальный получатель, в случае такой атаки, откроет подложное сообщение m и сошлётся на использование ассоциированного алгоритма вероятностного шифрования и случайного значения r'. Для того чтобы вычислить k из значения r придётся решить вычислительно сложную задачу дискретного логарифмирования, которые считается не решаемой при рекомендуемом значении p, тогда атакующий не сможет доказать, что шифртекст содержит какие либо другие сообщения, отличающиеся от m.

Предлагаемый протокол представляет интерес для практики ввиду следующих достоинств:

1) обеспечивает защиту от двусторонних атак;

2) достаточно высокое быстродействие (всего лишь в 2 раза медленнее алгоритма открытого шифрования 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 лишь 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.

Заключение. Предложен вычислительно эффективный протокол ОШ, реализуемый на практике. Содержащий механизмы аутентификации отправителя и ОШ. Стойкость к двусторонним атакам обеспечивается наличием ассоциированного алгоритма вероятностного шифрования, который порождает шифртекст, неотличимый от алгоритма ОШ. Протокол является стойким к атакам, когда нарушитель выдаёт себя за отправителя сообщения. Важным свойством протокола является использование стандартной инфраструктуры открытых ключей. Предложенный протокол разработан с использованием вычислительной сложности задачи дискретного логарифмирования в конечном поле $GF(p)$ и может быть реализован с использованием вычислений на эллиптических кривых, но это представляет тему отдельного исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption. Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, 1997. Vol. 1294. P. 90–104.
2. Bo Meng. A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext. Journal of Networks. 2009. Vol. 4. No. 5. P. 370–377.
3. Ishai Yu., Kushilevits E., Ostrovsky R. Efficient Non-interactive Secure Computation. Advances in Cryptology -- EUROCRYPT 2011. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, 2011. Vol. 6632. P. 406-425.
4. O'Neil A., Peikert C., Waters B. Bi-Deniable Public-Key Encryption. Advances in Cryptology – CRYPTO 2011. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, 2011. Vol. 6841. P. 525-542.
5. Klonowski M., Kubiak P., Kutyłowsk M. Practical Deniable Encryption // SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Nový Smokovec, Slovakia, January 19-25. 2008. P. 599-609.
6. Bo Meng, Jiang Qing Wang. A Receiver Deniable Encryption Scheme. Proceedings the 2009 International Symposium on Information Processing (ISOP'09), Huangshan, China, August 21-23, 2009 of Networks. 2009. P. 254–257.
7. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18–21
8. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи.: СПб.: БХВ-Петербург. – 2010.

УДК 681.3

ОТРИЦАЕМОЕ ШИФРОВАНИЕ: АЛГОРИТМЫ, ПРОТОКОЛЫ И ПРИМЕНЕНИЯ

Молдовян Александр Андреевич, Молдовян Николай Андреевич,
Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, В.О., 14-линия, д. 39,
e-mails: maa1305@yandex.ru; nmold@mail.ru

Аннотация: Рассматривается проблематика разработки прикладных алгоритмов и протоколов отрицаемого шифрования и их применение в современных средствах компьютерной безопасности. В качестве прикладных требований обосновывается вычислительная неотличимость от отрицаемого шифрования от вероятностного шифрования, использование стандартной инфраструктуры открытых ключей и достаточно высокая производительность алгоритмов и протоколов. Рассмотрены подходы к разработке схем отрицаемого шифрования различного типа, удовлетворяющих данным требованиям, и варианты их использования в средствах защиты информации.

Ключевые слова: *отрицаемое шифрование; шифрование с открытым ключом; вероятностное шифрование; защита информации, аутентификация.*

DENIABLE ENCRYPTION: MODERN ALGORITHMS AND APPLICATIONS

Moldovyan Alexander Andreevich, Moldovyan Nikolay Andreevich,
The St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
Russia, St. Petersburg, 14 line, the house 39
e-mails: maa1305@yandex.ru; nmold@mail.ru

Abstract: There are considered approaches to design practical algorithms and protocols for deniable encryption and its application in computer security systems. Computationally indistinguishable from

probabilistic encryption, using the standard public key infrastructure, and sufficiently high performance are justified as the criteria for designing deniable encryption algorithms and protocols.

Keywords: *deniable encryption; public-key encryption; probabilistic ciphering; information protection; entity authentication.*

Введение. Отрицаемое шифрование (ОШ) представляет собой криптографическое преобразование преобразуемых сообщений, которое формирует криптограмму с возможностью неоднозначного расшифрования, за счет чего обеспечивается возможность защиты передаваемой информации в случае принуждающих атак, когда отправитель сообщения и/или атакующий вынуждены раскрыть ключ шифрования и другие параметры, использованные в процессе зашифрования. В работе [1] показана принципиальная возможность выполнения ОШ при осуществлении шифрования по открытому ключу, а также с использованием разделяемого секретного ключа. Это соответствует двум основным типам алгоритмов и протоколов ОШ. По стойкости схемы ОШ разделяются на схемы, стойкие к принуждению 1) отправителя, 2) получателя (односторонние атаки) и 3) обеих сторон сеанса связи (двухсторонняя атака). В моделях принуждающих атак всегда принимается соглашение, что принуждение имеет место после того, как шифртекст был передан по каналу связи и перехвачен атакующим (точнее говоря, принимается соглашение, что имеет место перехват всех данных, переданных в ходе сеанса связи). В известной литературе по данной тематике основное внимание уделено разработке алгоритмов и протоколов ОШ с открытым ключом и схем ОШ использующих как открытые ключи, так и разделяемый секретный ключ. При этом предполагается, что атакующий, получая в свое распоряжение ключ шифрования, восстанавливает фиктивное сообщение, которое может иметь произвольное содержание по выбору отправителя или получателя. Часто протоколы ОШ строятся таким образом, что выбор фиктивного сообщения может быть осуществлен уже после передачи шифртекста по каналу связи. В этом случае в протоколе предусматривается наличие алгоритма подделки исходного сообщения, в качестве входных параметров которого задается шифртекст и фиктивное сообщение. Результатом выполнения алгоритма подделки является конкретные значения раскрываемых атакующему параметров, которые определяют восстановление из криптограммы выбранного фиктивного сообщения в ходе выполнения процедуры расшифрования. В протоколах такого типа должны быть предусмотрены согласованные действия отправителя и получатели в случае двухсторонней принуждающей атаке, поскольку успешная защита от такой атаки требует того, чтобы фиктивные сообщения, полученные по раскрытым данным отправителя и получателя, совпадали. Действительно, несовпадение означает то, что имеет место обман, а установление факта обмана должно приниматься за успешное выполнение атаки рассматриваемого типа.

Некоторые схемы ОШ устроены таким образом, что фиктивное сообщение выбирается заранее, а формирование шифртекста осуществляется путем совместного шифрования секретного и фиктивного сообщений. Это снимает вопрос о различиях фиктивных сообщений в случае двухсторонних атак. При таком построении может быть сокращен объем передаваемых данных в ходе защищенного сеанса связи для заданного фиксированного секретного сообщения. Недавно в работах [2], [3], [4], [5] дано обоснование требования вычислительной неотличимости ОШ от вероятностного шифрования для криптосхем с фиксированным фиктивным сообщением. Выполнение данного требования при разработке алгоритмов ОШ связано с обеспечением правдоподобия полного раскрытия атакующему параметров шифрования, что для принуждающих атак является немаловажным моментом.

В настоящем сообщении рассматриваются подходы к построению алгоритмов и протоколов ОШ, удовлетворяющих требованию вычислительной неотличимости от вероятностного шифрования, и обсуждается их применение как механизма защиты информации в информационно-телекоммуникационных системах,

Приложения отрицаемого шифрования. В известной литературе наиболее часто рассматриваются следующие направления применения протоколов ОШ: 1) обеспечение защиты от скупки голосов в системах тайного электронного голосования [6] и 2) реализация безопасных многосторонних вычислений [7]. Эти два направления практического применения ОШ представляются любопытными, но их реальное воплощение в рамках тех или иных технологий остается в настоящее время предметом дискуссий. На практике ОШ применено в ряде зарубежных средств компьютерной безопасности в качестве механизма защиты информации (например, в системах Best Crypt, FreeOTFE, True Crypt и др.). В последнем приложении используется упрощенная трактовка понятия ОШ по разделяемому секретному ключу, в которой отсутствует требование связи каждого бита шифртекста с каждым битом расшифрованного текста. В такой сравнительно наивной трактовке ОШ предполагается, что в случае принуждающей атаки раскрытию подлежит только часть шифртекста. Оставшаяся часть шифртекста объявляется случайными данными. При этом для шифрования используются два различных ключа и симметричные шифры обычного типа, например, AES.

Критическая оценка реализованного механизма шифрования показывает, что в упомянутых средствах компьютерной безопасности использование механизма ОШ носит формальный характер.

Правильнее было бы говорить, что шифрование по одному ключу использовано для создания стеганографического контейнера для хранения информации, зашифрованной на другом ключе. Фактически имеет место механизм защиты информации на основе комбинирования стеганографии и симметричного шифрования. Однако для защиты отдельных сообщений, которыми обмениваются удаленные пользователи, и отдельных файлов, хранимых в постоянной памяти ЭВМ, а также для построения защитных механизмов типа криптографических обманных ловушек, ориентированных на навязывание атакующему ложной информации, наивный подход к построению процедуры ОШ по разделяемому ключу представляется недостаточным. Действительно, наличие участков шифртекста, которые не используются для раскрытия фиктивного сообщения, дают атакующему существенные основания утверждать о неполноте раскрытия шифртекста.

Представляет интерес подход к устранение этого недостатка наивной трактовки понятия ОШ, состоящий в задании требования неотличимости шифртекста, полученного в результате ОШ от шифртекста, полученного в результате вероятностного шифрования фиктивного сообщения по фиктивному ключу. Задание этого требования потенциально расширяет области применения протоколов и алгоритмов ОШ, поскольку устраняет неполноту раскрытия шифртекста. Рассмотрение принуждающих атак, в которых для атакующего предполагается возможность измерения времени выполнения процедуры расшифрования или возможность доступа к машинному коду, реализующему эту процедуру, приводит к дополнительному требованию независимости процедуры расшифрования от ключа. То есть расшифрование шифртекста по секретному ключу и по фиктивному ключу должно выполняться с помощью одной и той же последовательности операций преобразования.

Разработка протоколов ОШ, удовлетворяющих принципу неотличимости от вероятностного шифрования, связана с использованием достаточно правдоподобного объяснения того, что размер шифртекста больше размера фиктивного сообщения, которое состоит в том, что атакующему дается разъяснение об использовании алгоритма шифрования вероятностного типа с целью получения более высокого уровня защищенности передаваемых сообщений. Рассмотрим различные типы алгоритмов отрицаемого шифрования, реализующими упомянутый принцип.

Использование блочных шифров в режиме отрицаемого шифрования. Для построения производительного алгоритма отрицаемого шифрования можно использовать идею объединения двух независимых шифртекстов, полученных шифрованием двух независимых сообщений с помощью одного о того же блочного шифра, в единую криптограмму таким образом, чтобы последняя была вычислительно неотличима от вероятностного шифрования одного из сообщений. Пусть разделяемый отправителем и получателем секретного сообщения ключ представляет собой две пары параметров $(K_1, \mu(x))$ и $(K_2, \lambda(x))$, где K_1 и K_2 – ключи блочного шифрования; $\mu(x)$ и $\lambda(x)$ – взаимно простые двоичные многочлены степени *n*. В протоколе отрицаемого шифрования пара $(K_1, \mu(x))$ рассматривается как секретный ключ, а пара $(K_2, \lambda(x))$ – как фиктивный ключ. Последняя пара также держится в секрете до тех пор, пока одна их сторон протокола или обе стороны не подвергнутся принуждающей атаке. Совместное шифрование секретного сообщения $T = (T_1, T_2, ...T_i ...T_z)$ и фиктивного сообщения $M = (M_1, M_2, ...M_i ...M_z)$, представленных в виде последовательности n-битовых блоков T_i и M_i ($i = 1,2,..., z$), соответственно, выполняется следующим образом.

1. Каждый i-тый блок данных T_i ($i = 1,2,..., z$) зашифровать по ключу K_1, используя формулу $C_{T_i} = E_{K_1}(T_i)$.

2. Каждый i-тый блок данных M_i зашифровать по ключу K_2: $C_{M_i} = E_{K_2}(M_i)$.

3. Для каждого значения $i = 1,2,..., z$ сформировать блок криптограммы C_i в виде битовой строки, представляющей двоичный многочлен, являющийся решением следующей системы линейных сравнений:

$$\begin{cases} C_i \equiv C_{T_i} \bmod \mu(x) \\ C_i \equiv C_{M_i} \bmod \lambda(x) \end{cases}, \qquad (1)$$

где блоки промежуточных шифртекстов C_{T_i} и C_{M_i} рассматриваются как двоичные многочлены.

4. Объединить блоки шифртекста C_i ($i = 1,2,..., z$) в единую криптограмму $C = (C_1, C_2, ...C_i ...C_z)$.

При формировании блоков шифртекста C_i выполняются вычисления в конечных кольцах двоичных многочленов. В соответствии с китайской теоремой об остатках решение системы сравнений (1)

представляет собой двоичный многочлен степени $2n$, который вычисляется по формуле

$$C_i = \left\{C_{T_i}\lambda(x)\left[\lambda^{-1}(x)\bmod\mu(x)\right] + C_{M_i}\mu(x)\left[\mu^{-1}(x)\bmod\lambda(x)\right]\right\}\bmod\mu(x)\lambda(x).$$

Вычисление многочленов $\lambda^{-1}(x)\bmod\mu(x)$ и $\mu^{-1}(x)\bmod\lambda(x)$ может быть осуществлено заранее, например, при генерации секретного ключа, что позволит повысить скорость шифрования, обеспечиваемой этим алгоритмом. Основной вклад в вычислительную трудоемкость шага 3 вносит операция деления на многочлен, равный произведению $\mu(x)\lambda(x)$. Увеличение производительности за счет выбора в качестве модулей $\mu(x)$ и $\lambda(x)$ многочленов с малым числом ненулевых коэффициентов, например, двоичных трехчленной неприемлемо, поскольку эти многочлены включаются как элементы разделяемого секрета.

Все возможные остатки от деления на модуль $\mu(x)\lambda(x)$, являющийся двоичным многочленом степени $2n+2$, представляют собой двоичные многочлены, степень которых равна или меньше значения $2n+1$, т.е. все возможные остатки представляют собой множество битовых строк длины $2n$. Таким образом, рассмотренный алгоритм отрицаемого шифрования генерирует криптограмму, размер которой в точности равен сумме размеров шифруемых сообщений.

В качестве используемого блочного шифра можно применить как известные блочные шифры, так и разрабатываемые специально для реализации протоколов отрицаемого шифрования. Алгоритм отрицаемого шифрования с использованием решения системы двух линейных сравнений по взаимно простым модулям $\mu(x)$ и $\lambda(x)$ можно отнести к алгоритмам блочного совместного шифрования пары сообщений. Действительно, любой случайный $(2n)$-битовый блок шифртекста однозначно расшифровывается по разделяемому ключу, т.е. между множеством $(2n)$-битовых блоков и множеством пар n-битовых блоков процедура совместного шифрования двух n-битовых блоков данных устанавливает взаимно однозначное соответствие (при заданном фиксированном ключе).

При шифровании с помощью рассмотренного в этом разделе алгоритма отрицаемого шифрования сообщений произвольной длины последние разбиваются на блоки, которые могут шифроваться в режиме электронной кодовой книги (независимое шифрование пар входных блоков данных), в режиме сцепления блоков шифра или в других известных и применяемых для блочных шифров режимах, которые могут быть соответствующим образом адаптированы для случая отрицаемого шифрования.

Ассоциируемый алгоритм вероятностного шифрования описывается следующим образом:

1. Каждый i-тый блок данных M_i ($i = 1,2,...,z$) зашифровать по ключу K_2, используя формулу $C_{M_i} = E_{K_2}(M_i)$.

2. Сгенерировать случайный двоичный многочлен $\mathrm{P}(x)$ степени $2n-1$ (т.е. случайную n-битовую строку) и случайный неприводимый многочлен $\rho(x)$ степени n.

3. Для каждого значения $i = 1,2,...,z$ сформировать блок криптограммы C_i в виде битовой строки, представляющей двоичный многочлен, являющийся решением следующей системы линейных сравнений:

$$\begin{cases} C_i \equiv C_{M_i} \bmod\lambda(x) \\ C_i \equiv \mathrm{P}(x)\bmod\rho(x) \end{cases}. \qquad (2)$$

4. Объединить блоки шифртекста C_i ($i = 1,2,...,z$) в единую криптограмму

$$C = (C_1, C_2, ...C_i...C_z).$$

Произвольный заданный $(2n)$-битовый блок C_i может быть получен с помощью ассоциированного алгоритма вероятностного шифрования, выбирая различные неприводимые двоичные многочлены степени n в качестве многочлена $\rho(x)$. Действительно, выбор произвольного неприводимого многочлена $\rho(x)$, имеющего степень n, задает значение многочлена $\mathrm{P}(x) \equiv C_i \bmod\rho(x)$, при подстановке которого в (2) вместе с выбранным $\rho(x)$) определяет то, что заданный блок C_i будет единственным решением (2) (Этот ассоциируемый алгоритм является примером вероятностных шифров, для которых в ходе выполнения процедуры расшифрования не имеет места однозначное восстановление случайных значений, использованных в процессе зашифрования).

Наличие алгоритма вероятностного шифрования, который с конечной вероятностью может

преобразовать фиктивное сообщение M в криптограмму C, обосновывает утверждение отправителя и получателя, подвергаемых атаке с принуждением, о том, что только раскрываемый ими ключ $(K_2, \lambda(x))$ и сообщение M составляют полный секрет, связанный с имевшим место сеансом секретной связи. Чтобы уличить отправителя и/или получателя секретного сообщения, атакующему нужно показать, что криптограмма содержит, кроме сообщения M, также и другое осмысленное сообщение, т.е. нужно взломать блочную шифрующую функцию E, причем использованную в режиме вероятностного шифрования, который улучшает статистические свойства генерируемого шифртекста.

Расшифрование криптограммы $C = (C_1, C_2, ...C_i ...C_z)$ по фиктивному ключу $(K_2, \lambda(x))$ выполняется по следующему алгоритму, который одновременно является и алгоритмом расшифрования, соответствующим ассоциированному алгоритму вероятностного шифрования:

1. По каждому блоку C_i ($i = 1,2,..., z$) восстановить блок промежуточного шифртекста C_{M_i} по формуле $C_{M_i} \equiv C_i \bmod \lambda(x)$.

2. Для $i = 1,2,..., z$ восстановить блоки исходного сообщения M_i по формуле $M_i = E_{K_2}^{-1}(C_{M_i})$.

Расшифрование криптограммы C по секретному ключу $(K_1, \mu(x))$ также выполняется по последнему алгоритму. При этом на выходе алгоритма будет получено секретное сообщение $T = (T_1, T_2, ...T_i ...T_z)$.

Другим подходом к реализации режима отрицаемого шифрования для блочных шифров является формирование объединенных блоков C_i по парам блоков промежуточных шифртекстов C_{T_i} и C_{M_i} путем решения системы из двух линейных уравнений, коэффициенты которой задаются по ключам K_1 и K_2 по аналогии со способом, описанным в работе [4].

Подходы к построению скоростных алгоритмов ОШ поточного типа предложены в работах [8], [9]. Алгоритмы ОШ поточного типа представляют практический интерес для защиты файлов в компьютерных системах, а также сообщений в телекоммуникационных системах, включая речевые сообщения. Недавно показана возможность построения коммутативных алгоритмов ОШ [10].

Протоколы отрицаемого шифрования по открытому ключу. Для реализации протоколов данного типа используются различные подходы, однако во многих случаях описанные в литературе протоколы ОШ не являются практичными, поскольку обладают недостаточной производительностью или не обеспечивают требуемой стойкости. В работах [4], [11] для построения практичных протоколов ОШ по открытому ключу предложен подход, в котором в рамках протокола используется процедура взаимной аутентификации отправителя и получателя секретного сообщения по их открытым ключам, в ходе которой одновременно реализуется взаимный обмен разовыми открытыми ключами. Последние используются для шифрования секретного сообщения, а зарегистрированные открытые ключи – для шифрования фиктивного сообщения. Для построения протоколов ОШ в соответствии с таким подходом может быть использована стандартная инфраструктура открытых ключей, которая имеет достаточно широкое практическое применение в технологиях цифровой подписи. Это существенно дополняет преимущества высокой стойкости и производительности.

Практический интерес представляют комбинированные протоколы ОШ, в которых используется открытый ключ получателя и разделяемый секретный ключ. В случае атаки с принуждением отправитель и получатель сообщения утверждают, что для шифрования был использован вероятностный алгоритм открытого шифрования. В рамках такого построения легко обеспечивается высокая стойкость протокола и достаточное его быстродействие, однако алгоритм расшифрования секретного и фиктивного сообщений имеют существенные различия, что может быть использовано в специальных типах принуждающих атак.

Одно из направлений построения протоколов ОШ связано с использованием алгоритмов открытого шифрования, представляющих собой генерацию квадратных или кубичных сравнений по трудно разложимому модулю [12].

Заключение. В качестве нового механизма защиты информации в информационно-телекоммуникационных системах представляет интерес использование протоколов ОШ с открытым ключом и с разделяемым секретным ключом. В настоящее время в известной литературе описаны подходы к построению алгоритмов и протоколов ОШ, удовлетворяющие основным критериям, требуемым для их практического использования.

СПИСОК ЛИТЕРАТУРЫ

1. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption. Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, 1997. Vol. 1294. P. 90–104.
2. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопросы защиты

информации. 2013. № 2. С. 18-21.
3. Морозова Е.В., Мондикова Я.А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. № 6. 2013. С. 73-78.
4. Moldovyan A.A., Moldovyan N.A. Practical Method for Bi-Deniable Public-Key Encryption // Quasigroups and related systems. 2014. Vol. 22. P. 277-282.
5. Молдовян Н.А., Молдовян Д.Н., Вайчикаускас М.А. Генерация кубичных уравнений как способ открытого шифрования // Вопросы защиты информации. 2015. № 2. С. 3-7.
6. Bo Meng. A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext. Journal of Networks. 2009. Vol. 4. No5. P. 370–377.
7. Ishai Yu., Kushilevits E., Ostrovsky R. Efficient Non-interactive Secure Computation. Advances in Cryptology – EUROCRYPT 2011. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, 2011. Vol. 6632. P. 406-425.
8. . Березин А.Н., Молдовян Н. А., Молдовян А. А. Потоковое отрицаемое шифрование, вычислительно неотличимое от вероятностного шифрования // XVIII Международная конференция по мягким вычислениям и измерениям (SCM'2015), Санкт-Петербург, 19 – 21 мая 2015 г. / Труды конференции. СПб, СПбГЭТУ «ЛЭТИ», 2015. С. 95-99.
9. Moldovyan A.A., Moldovyan D.N., Shcherbacov V.A. Stream Deiable-Encryption Algorithm Satisfying Criterion of the Computational Indistinguishability from Probabilistic Ciphering, Workshop on Foundations of Informatics, August 24-29, 2015, Chisinau, Proceedings, p. 318-330.
10. Костина А.А., Молдовян Н.А., Морозова Е.В. Коммутативный алгоритм отрицаемого шифрования на основе трудности задачи дискретного логарифмирования // Нелинейный мир. 2014. Т. 12. № 5. С. 59-62.
11. Moldovyan A. A., Moldovyan N. A., Shcherbakov V. A. Bi-Deniable Public-Key Encryption Protocol Secure Against Active Coercive Adversary // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2014. № 3 (76). P. 23-29.
12. Moldovyan N.A., Moldovyan A.A., Shcherbacov V.A. Provably sender-deniable encryption scheme // Computer Science Journal of Moldova/ 2015, V.23. № 1(67). P. 62-71.

УДК 004.056.5

ОЦЕНКА СКОРОСТНЫХ ХАРАКТЕРИСТИК РЕАЛИЗАЦИИ АТАКИ ТИПА ПЕРЕБОР ПАРОЛЯ НА IP-АТС ПРИ ИСПОЛЬЗОВАНИИ FAIL2BAN

Молдовян Александр Андреевич[1], Ковцур Максим Михайлович[2],
[1] Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, В.О., 14-линия, д. 39,
[2] Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков д.22, корп.1,
e-mails: maa1305@yandex.ru, maxkovzur@mail.ru

Аннотация: В статье рассмотрены временные параметры атаки перебор пароля на IP-АТС, представлены ограничения, играющие решающую роль на скорость реализации данной атаки. Приведено описание инструмента для защиты от атаки Fail2BAN, а также рекомендации по выбору значений параметров – времени блокировки и числа неудачных попыток регистрации – в зависимости от скорости канала связи, а также производительности IP-АТС.

Ключевые слова: *IP-АТС; IP-телефония; перебор пароля; Fail2Ban.*

EVALUATION OF SPEED CHARACTERISTICS OF BRUTE FORCE PASSWORD ATTACK TO IP-PBX WHEN USING FAIL2BAN

Moldovyan Alexander Andreevich[1], Kovtsur Maxim Mihaylovich[2],
[1] St.Petersburg institute for informatics and automation
of the Russian academy of sciences,
Russia, St. Petersburg, 14 line, the house 39,
[2] Federal State Educational Budget-Financed Institution of Higher Vocational Education
The Bonch-Bruevich Saint - Petersburg State University of Telecommunications,
Russia, St. Petersburg, pr. Bolsheviks d.22, building 1,
e-mails: maa1305@yandex.ru, maxkovzur@mail.ru

Abstract: The article describes the timing characteristics of the brute force password attack to IP-PBX. Limitations, which play an important role in the speed of implementation of this attack, are presented. The Fail2BAN utility's description is presented. Prepared recommendations for the selection of values – the blocking time and the number of failed login attempts – depending on the speed of the communication channel and performance of the IP-PBX.

Keywords: *IP-PBX, IP-telephony; brute force password; Fail2Ban.*

Введение. 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 на IP-АТС. Для защиты АТС от данной атаки распространено использование инструмента Fail2BAN [1]. Обеспечению безопасности IP-телефонии посвящено много статей, в том числе [2], [3], [4] и др. Однако, отсутствуют обоснования по

выбору значений параметров для приложения Fail2Ban. Целью данной работы является формирование рекомендаций для выбора значений параметров этого приложения, а также оценка скорости реализации атаки перебора пароля при использовании Fail2Ban. Возможная схема организации сети IP-телефонии приведена на рисунке 1. Одним из распространенных бесплатных решений для корпоративной IP-телефонии является платформа Elastix [5], основанная на программной IP-АТС Asterisk и содержащая большое число дополнительных модулей, в том числе модулей для обеспечения информационной безопасности. Одним из таких модулей является Fail2Ban [6].

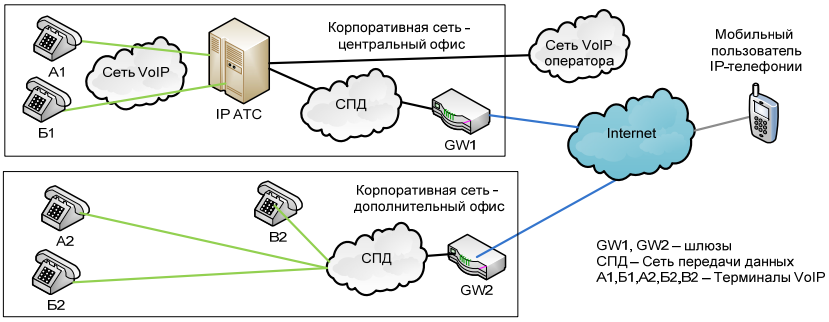


Рис. 1. Структурная схема сети IP-телефонии

Наличие мобильных пользователей требует организации доступности ресурсов IP-АТС из глобальной сети, что приводит к возможности реализации атаки перебор пароля на АТС для захвата ресурсов. Для регистрации на телефонной станции VoIP-клиент использует процедуру, представленную в RFC3261 [7], приведенную на рисунке 2. В результате регистрации пользователь и IP-АТС обмениваются четырьмя сообщениями. Оценка влияния регистраций на функционирование телефонной сети рассмотрена в [8], однако не уделено внимания регистрациям, вызванным атакой перебор пароля.

Рис. 2. Авторизация пользователя на IP-АТС

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 $C_{TX}, C_{RX}, C_{CPU}, C_{F2B}, C_{HAP}$, где:

C_{TX}, бит/с – максимальная допустимая скорость передачи согласно тарифному плану владельца IP-АТС;

C_{RX}, бит/с – максимальная допустимая скорость приема согласно тарифному плану владельца IP-АТС;

C_{CPU}, регистраций/с – максимально возможное число регистраций в секунду, поддерживаемое IP-АТС, которое зависит от используемого программного и аппаратного обеспечения АТС, производительности процессора, а также дополнительных настроек;

C_{F2B}, регистраций/с – максимально допустимое число регистраций с учетом ограничений Fail2ban, *позволяющего* блокировать на время $T_{БЛ}$ нарушителей, выполняющих атаку перебор пароля и не подобравших пароль более Q раз;

C_{HAP}, *регистраций*/с – максимальная возможная скорость перебора пароля при выполнении регистраций со стороны активного нарушителя, определяемая его возможностями, техническим обеспечением и дополнительными факторами.

Итоговая скорость перебора пароля будет соответствовать числу регистраций в секунду C_{Π} и определяться, как:

$$C_{\Pi} = \min(C_{NTX}, C_{RTX}, C_{CPU}, C_{F2B}, C_{HAP}) \text{, регистраций/с,} \quad (1)$$

где:

$$C_{NTX} = \frac{C_{TX}}{N_{NTX}},$$

где

N_{TX}, бит –объем данных, передаваемый АТС при обработке одного запроса на регистрацию;

$$C_{NRX} = \frac{C_{RX}}{N_{NRX}},$$

где

N_{RX}, бит – объем данных, принимаемый АТС от терминала IP-телефонии при обработке одного запроса на регистрацию;

C_{F2B}, регистраций/с – скорость регистраций, ограниченная приложением Fail2BAN.

Следует отметить, что выделяется два значения $C_{CPU} : C_{CPUDDOS}$ – пороговое значение C_{CPU}, при превышении которого IP-АТС будет отбрасывать дополнительные поступающие сообщения без их обработки из-за нехватки вычислительных мощностей, и C_{CPUMAX} – значение скорости перебора, при котором предоставление базового набора сервисов будет продолжаться. В рамках исследования введем допущение, что основная цель нарушителя – реализация успешного перебора пароля. Поэтому атака будет проводиться со скоростью $C_{CPU} = C_{CPUMAX}$. При дальнейшем анализе будем полагать, что нарушитель имеет неограниченную C_{HAP}, а также имеет контроль над N_{IP} хостами для выполнения атаки. Также введем допущение, что владелец IP-АТС имеет симметричный канал передачи данных со скоростью $C = C_{TX} = C_{RX}$ к глобальной сети, характеристики которого лежат в диапазоне 1 Мбит/с – 100 Мбит/с.

Выполним оценку граничного значения C_{CPU}, при котором скорость перебора будет ограничиваться значением C и не будет ограничиваться производительностью IP-АТС.

$$C_{CPU} > \frac{C}{N_{TX}} \quad (2)$$

$$C_{CPU} > \frac{C}{N_{RX}} \quad (3)$$

Для оценки N_{TX} и N_{RX} проведен эксперимент, схема которого представлена на рисунке 3. В качестве IP-АТС выбрана платформа Elastix [5]. К управляемому коммутатору подключались компьютер с IP-АТС, компьютер ПК2 с установленным сетевым анализатором пакетов Wireshark, а также компьютеры ПК3 – ПК6 с установленными программными VoIP клиентами и несколько аппаратных VoIP терминалов. Клиенты выполняли регистрацию на IP-АТС, пакеты зеркалировались с помощью коммутатора на порт подключения ПК2, где выполнялась оценка объема сообщений.

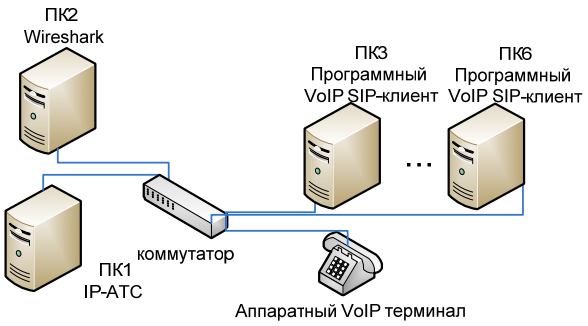


Рис. 3. Экспериментальная оценка регистрационных данных VoIP

Результаты экспериментальной оценки приведены в таблице 1.

Таблица 1

Экспериментальная оценка N_{TX} и N_{RX}

Название VoIP клиента	N_{TX} (бит)	N_{RX} (бит)
PhonerLight	10224	11640
Phoner.de	9152	10816
3CX mobile client	9824	11088
Linksys SPA3102	9720	10184
Zyxel P2300RDL	9752	8776
Усредненное значение	9734,4	10500,8

Очевидно, что минимальное значение из C_{NTX}, C_{NRX} будет определяться N_{RX}. Соответственно, исходя из (1), C_{CPU} будет определяться (3). Зависимость C_{CPU} от C представлена на рисунке 3. Для оценки значения C_{CPU} также был выполнен эксперимент, схема которого представлена на рисунке 4. В ходе эксперимента на ПК3-ПК6 запускались приложения, отправляющие на ПК1 запросы на регистрацию с высокой скоростью. При 400 одновременных запросах на регистрацию загрузка центрального процессора IP-АТС достигала 25%, а при 1200 одновременных запросах – 90%.

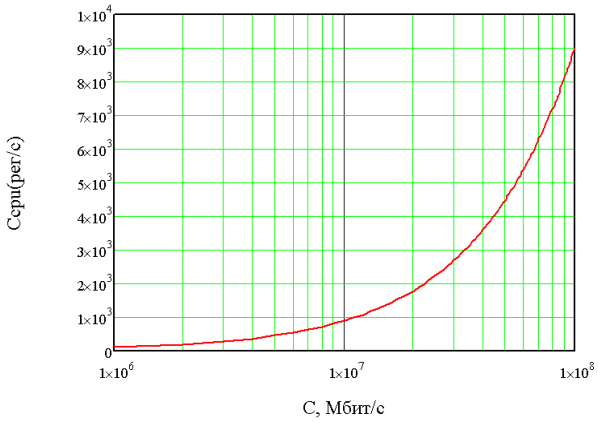


Рис. 4. Зависимость граничного значения C_{CPU} от C

Однако, в случае ограничения $C_{П}$ по причине C или C_{cpu} – будут возникать проблемы при оказании сервисов легитимным пользователям. Поэтому целесообразно учитывать значения запаса $C_{cpu_зап}$ и $C_{c_зап}$ такие, что:

$$C_{cpu_зап} = C_n - C_{CPU} \quad (4)$$

$$C_{c_зап} = C_n - \frac{C}{N_{rx}} \quad (5)$$

$C_{CPU\ ЗАП}$ и $C_{C\ ЗАП}$ требуют дополнительной оценки.

В рамках исследования предлагается задать $C_{CPU\ ЗАП} = 0{,}5C_{CPU}$, а $C_{C\ ЗАП} = n\,k + N_{RX}$, где:

n – число одновременных разговоров;

k, бит/с – скорость канала связи, необходимая для обслуживания одного разговора;

r – число одновременных регистраций в секунду от легитимных пользователей.

Одним из инструментов, используемых для защиты от атаки перебора пароля, является приложение Fail2Ban. Пользователь настраивает параметры $T_{БЛ}$ и Q. В этом случае, если хост выполняет Q неуспешных попыток авторизации, он блокируется приложением на время $T_{БЛ}$ средствами Linux Iptables. Правила блокировки создаются автоматически средствами Fail2Ban и удаляются через $T_{БЛ}$ секунд.

Согласно данным в источниках массовой информации, бот-нет сети могут достигать размера от нескольких десятков до сотен тысяч компьютеров [9],[10]. При этом очевидно, нарушитель, имеющий цель получить доступ к ресурсам IP-АТС, располагающий доступом к управлению такой сетью, будет

реализовывать поэтапный перебор пароля, при котором хосты будут выполнять атаки поочередно группами, чтоб наиболее эффективно использовать доступный ресурс. Тогда C_{F2B} будет иметь вид:

$$C_{F2B} = \frac{N_{IP}Q}{T_{БЛ}}, \text{ регистраций/с,} \quad (6)$$

где

N_{IP} – число разных хостов, с которых нарушитель может выполнять атаку перебор пароля,

Q – число некорректных попыток регистрации, через которое включается блокировка Fail2Ban,

$T_{БЛ}$,с – время блокировки хоста нарушителя, выполнившего некорректную регистрацию более Q попыток.

На число N_{IP} пользователь не может оказывать влияния. В этом случае, при расчетах зададимся возможным известным значением N_{IP}, которое может использовать нарушитель. Значение C_{CPU} также формируется индивидуально для каждой АТС и может быть определено пользователем самостоятельно. Зададимся C_{CPU}=1000 регистраций/с, N_{IP}=10000. Тогда в соответствии с (6) следует выбирать такие значения $T_{БЛ}$ и Q, при которых

$$C_{CPU} + C_{CPU_ЗАП} > \frac{N_{IP}Q}{T_{БЛ}} \text{ и } C + C_{C_ЗАП} > \frac{N_{IP}QN_{RX}}{T_{БЛ}},$$

где

$C_{CPU_ЗАП}$, регистраций/с – запас по производительности для обслуживания нормальной текущей нагрузки IP-АТС,

$C_{ЗАП}$, запросов/с – запас по полосе пропускания канала связи, необходимый для обслуживания нормальной текущей нагрузки IP-АТС.

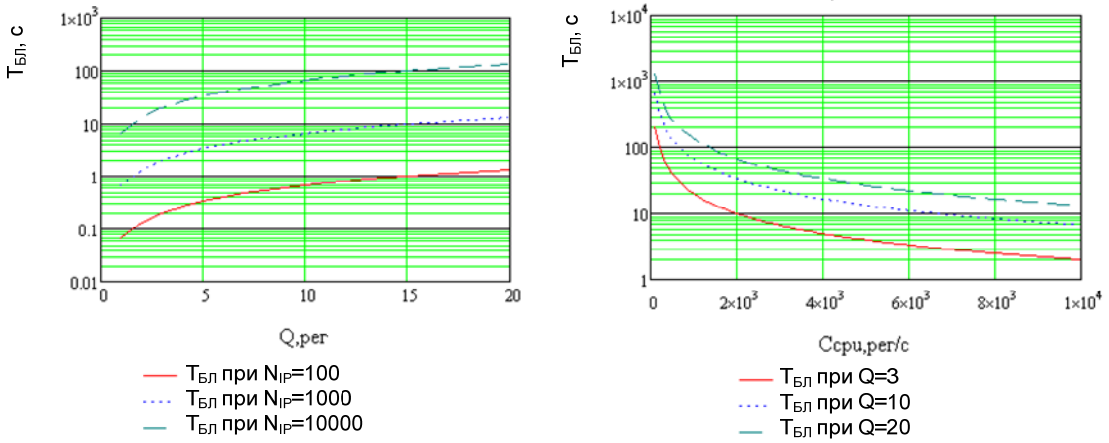
В этом случае при атаке перебора пароля IP-АТС не будет испытывать перегрузки и атака не отразиться на предоставляемых при нормальной работе сервисах.

$$T_{БЛ} > \frac{N_{IP}Q}{C_{CPU} + C_{CPU_ЗАП}}, \quad (7)$$

$$T_{БЛ} > \frac{N_{IP}QN_{RX}}{C + C_{C_ЗАП}}. \quad (8)$$

Определим значения $T_{бл}$, соответствующие различным значением Q и выражениям (6–7). Полученные зависимости представлены на графиках на рисунке 5.

Так при N_{IP} *=10000,* C_{CPU} *=1000* регистраций*/с,* Q *=5,* $T_{БЛ}$ следует выбирать $T_{БЛ}$ *>30 с.* Увеличение времени ожидания позволяет сократить нагрузку на CPU при обработке запросов, направленных на перебор пароля. Однако, установка слишком длительного времени может привлечь к длительной блокировке легитимных пользователей, выполняющих перенастройку оборудования.



а) б)

Рис. 5. Зависимость $T_{БЛ}$ а) от N_{IP} б) от C_{cpu}

Заключение. В статье представлена структурная схема сети IP-телефонии предприятия, а также приведены рекомендации по выбору параметров для приложения Fail2Ban, используемому для ограничения скорости атаки типа перебор пароля.

Исследование показало, что выбор опций необходимо осуществлять, основываясь не только на производительности IP-АТС, но и на скорости имеющегося канала связи. Составлена аналитическая зависимость параметра $T_{БЛ}$ от Q, N_{IP} и C_{CPU}. Однако – дальнейшего исследования требует оценка влияния большого числа правил, созданных за счет работы Fail2Ban, на CPU во время функционирования IP-АТС.

СПИСОК ЛИТЕРАТУРЫ

1. Обеспечиваем безопасность VoIP-сервиса и защиту от прослушивания // Хакер. 2013. № 12(179). С. 134-140.
2. Ковцур М.М. Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии // Фундаментальные исследования. 2014. № 8 (часть 6). С. 1300-1308.
3. Дербина Е.А., Щербаков А.В. Оценка уязвимостей Voice-Over-IP протоколов // Молодежный научно-технический вестник. 2015. № 8. URL: http://sntbul.bmstu.ru/doc/790542.html (дата обращения 25.08.2015).
4. Докучаев В.А., Шведов А.В. Защита информации на корпоративных сетях VoIP // Электросвязь. 2012. № 4. С. 5-8.
5. Elastix. Open Source Unified Communications Server. URL: http://www.elastix.org/index.php/en/ (дата обращения 27.08.2015)
6. Fail2ban. URL: http://www.fail2ban.org/wiki/index.php/Main_Page (дата обращения 27.08.2015).
7. Request for Comments: 3261 SIP: Session Initiation Protocol. URL: https://www.ietf.org/rfc/rfc3261.txt (дата обращения 29.07.2015).
8. Журавлев С.В. Влияние процедуры регистрации пользовательского SIP-оборудования на функционирование телефонной сети общего пользования // T-Comm - Телекоммуникации и Транспорт. 2011. № 7. С. 76-79.
9. Обнаружена бот-сеть из 200 000 мобильных устройств [Электронный ресурс] // Сайт компании Dr.Web. URL: http://news.drweb.ru/show/?i=3929&lng=ru&c=14 (дата обращения 21.08.2015).
10. 2015 Internet Security Threat Report. Volume 20. Symantec Corporation. URL: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf (дата обращения 25.08.2015).

ГРНТИ 81.93.29

УНИЧТОЖЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Насретдинова Диана Рамилевна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, ул. Кронвергский проспект, д. 49,
e-mail: ya.diana258@yandex.ru

Аннотация: В статье рассмотрены этаны работы экспертной комиссии, методы уничтожения конфиденциальной информации, такие как: сжигание, химическое уничтожение, шредирование. Выявлены недостатки каждого из методов.

Ключевые слова: *экспертная комиссия; конфиденциальные документы; сжигание; шредирование; химическая обработка.*

CONFIDENTIAL DOCUMENT DESTRUCTION

Nasretdinova Diana Ramilena,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: ya.diana258@yandex.ru

Abstract: In the article atany work of the expert Commission, methods of destruction of confidential information, such as incineration, chemical destruction, turnings shredding. Identified shortcomings of each method.

Keywords: *the expert Commission; confidential documents; burning; turnings shredding; chemical treatment.*

Введение. Во многих государственных министерствах, силовых ведомствах и некоторых коммерческих организациях существует определенный вид документации, который содержит информацию ограниченного доступа. В данном случае носители информации с таким родом сведений подлежат уничтожению как секретные документы. К их иничтожению предъявляются высокие требования, которые должны обеспечивать безопасность и конфиденциальность процедуры.

На сегодняшний день можно заметить, что 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, на которую и возлагаются обязанности по отнесению информации к актуальной или устаревшей.

В результате проведения процедуры оценки выделяются четыре категории дел:

1. Дела постоянного хранения, подлежащие в последующем передаче в государственный архив.
2. Дела долговременного хранения в ведомственном архиве учреждения, фирмы (свыше 10 лет).
3. Дела временного хранения (до 10 лет).
4. Дела, подлежащие уничтожению в связи с истечением срока хранения.

В процессе уничтожения конфиденциальных материалов должен быть установлен определенный порядок, который исключает возможность изучения документов посторонними лицами.

Уничтожение документов – процедура сложная, и требует максимального внимания и ответственности, так как в ходе уничтожения конфиденциальных документов могут возникнуть 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 [2].

Перечисленные факторы возникновения угроз можно избежать при соблюдении обязательных правил уничтожения документов, дел и носителей информации:

1. Коллегиальность и профессионализм принятия решения об уничтожении документов, дел и самого процесса уничтожения; документирование каждого этапа подготовки к уничтожению и уничтожение документов и дел;
2. Внесение комиссией отметок об уничтожении в акт и учетные формы только после фактического уничтожения документов и дел.

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 и подписывается всеми членами комиссии.

Процесс уничтожения конфиденциальных документов и носителей информации состоит из последовательно выполняемых процедур:

1. Подготовку документов, дел и носителей информации к уничтожению;
2. Оформление акта на уничтожение;
3. Уничтожение документов по акту.

Основные способы уничтожения бумажных документов:

- шредирование,
- сжигание,
- химическая обработка.

Каждый из выше представленных способов имеет свои положительные и отрицательные качества, и используется в зависимости от конкретного делопроизводства, законодательства и возможностей определенной организации [3].

Сжигание на протяжении многих лет было самым эффективным и популярным методом уничтожения бумажных документов. Основным достоинством, которым обладает данный метод – это его простота и дешевизна, при правильном применении технологии гарантируется полное уничтожение информации, и, в крайнем случае, можно обойтись подручными средствами, без использования сложного дополнительного оборудования.

Так же он имеет определенные недостатки:

- для уничтожения большого количества документов необходимо затратить время и обеспечить непрерывный контроль со стороны исполнителей, т.к. бумага и горит хорошо, но может сгореть не до конца, что может привести к непроизвольному разглашению информации;
- сжигать документы необходимо только с применением специального оборудования (например, в котельной). Если процедура будет производиться на открытой местности (например, на костре), то ветер будет разносить полуобгоревшие документы на неопределенное расстояние;
- на сегодняшний день сжигание считается экологически вредным методом уничтожения из-за столбов дыма и загрязнения воздуха, от которого постепенно отказываются во многих странах мира.

Одним из менее распространённых методов является химическая обработка. Процесс очень прост, но требует подготовки, так как неумелое использования средств может привести к повреждения участков кожи человека. В процессе химической обработке совершается размягчение бумаги и превращение ее в бумажную массу. Это самый надежный, но недешевый метод, и в настоящее время его используют в качестве дополнительной меры безопасности после шредирования секретных документов.

У метода имеются свои недостатки:

- требуется специальное оборудование;
- процесс уничтожения время затратный и имеется определенный риск несанкционированного доступа к информации;

– вследствие длительности процесса необходимо присутствие уполномоченного лица при уничтожении конфиденциальных документов от начала и до завершения процедуры уничтожения, что в ствою очередь затруднительно.

Шредирование – наиболее распространенный и популярный метод уничтожения бумажных документов. Привлекают его дешевизна, «экологичность», достаточная надежность.

Главное достоинство – документы можно уничтожать постепенно, не покидая пределы территории, так же не требуется выделять много места для временного хранения отобранных на уничтожение материалов. Недостатком является то, что если документы, уничтоженные шредером, попадут целенаправленному и выносливому злоумышленнику, то он сможет их восстановить [1].

Организации или самостоятельно уничтожают документы, или пользуются услугами фирм, занимающихся переработкой вторичных отходов.

Заключение. 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.

СПИСОК ЛИТЕРАТУРЫ

1. Алексенцев А.И. Понятие и сфера действия конфиденциального делопроизводства // Секретарь-референт. № 1. 2002
2. Типовая инструкция по делопроизводству в Федеральных органах исполнительной власти, утверждённая приказом Федеральной архивной службы России от 27.11.2000 № 68.
3. Стенюков М.В. Документы. Делопроизводство. – М.; «Приор», (издание 9-е переработанное и дополненное), 2005. – 160 с.

УДК 004.056

ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ДЕСТРУКТИВНЫХ СОСТОЯНИЙ И ПЕРЕХОДОВ

Нурдинов Руслан Артурович,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверский пр., д. 49,
e-mail: nurdinov.ra@mail.ru

Аннотация: в статье представлена модель оценки рисков безопасности информационной системы. Определены множества деструктивных состояний для типов компонентов информационной системы: информационных активов, программного обеспечения, технических средств и каналов связи. Переход компонента информационной системы в деструктивное состояние возможен в результате действий источников угроз, либо при переходе связанного компонента в деструктивное состояние. Разработанная модель позволяет осуществлять динамическую детализированную оценку рисков безопасности информационной системы. Эксперты могут принимать участие в обучении модели, однако их постоянное участие в процессе оценки рисков не требуется.

Ключевые слова: *информационная система, угроза информационной безопасности, оценка рисков, эффективность защитных мер, модель состояний и переходов.*

INFORMATION SYSTEM SECURITY RISK ASSESSMENT BASED ON STATES AND TRANSITIONS MODEL

Nurdinov Ruslan,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: nurdinov.ra@mail.ru

Abstract: the article presents information security risk assessment model. It is defined sets of destructive states for information system components types: information assets, software, hardware and data channels. Transition of information system component to the destructive state is possible as a result of threats sources actions or if there was a related component transition to the destructive state. The developed model is allows for dynamic detailed information system security risk assessment. Experts can participate in the model training, but their continued involvement in the process of risk assessment is not required.

Keywords: *Information system, information security threat, risk assessment, countermeasures effectiveness, states and transitions model.*

Введение. 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 [6]. 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 трудоёмкой и трудновыполнимой. Под словом «динамическая» подразумевается возможность проведения постоянной переоценки рисков при изменении входных данных, а под словом «детализированная» – осуществление оценки рисков на уровне отдельных информационных активов (ИА), экземпляров программного обеспечения (ПО) и технических средств (ТС). Чаще всего оценка рисков информационной безопасности (ИБ) проводится слишком грубо (с использованием качественных шкал, шаблонизирования оценок), что снижает интерес к риск-ориентированному подходу как среди специалистов ИБ, так и среди представителей топ-менеджмента компаний.

Целью исследования является разработка детализированной динамической модели оценки рисков безопасности информационной системы.

Оценка рисков безопасности информационной системы. Под риском информационной безопасности понимается измерение комбинации вероятности случая и его последствий [8]. Риск может оцениваться как качественно, так и количественно (в стоимостном выражении). Наиболее распространенной на практике остается качественная оценка рисков, когда при отсутствии точных данных значения элементов риска устанавливает проводящий анализ рисков эксперт по заданным качественным шкалам. Для количественной оценки рисков требуется очень большой объем исходных данных, вследствие чего прогнозирование отдельных элементов риска с приемлемой точностью является весьма трудоёмкой и трудновыполнимой задачей. Однако, только количественная оценка позволяет сопоставить выгоду от использования защитных мер с затратами на их реализацию и эксплуатацию [0].

Количественная оценка риска осуществляется по формуле:

$$R = P_T \cdot P_V \cdot Q \tag{1}$$

где

R – риск,

P_T – вероятность возникновения угрозы,

P_V – вероятность использования уязвимости,

Q – ущерб или затраты в результате реализации угрозы.

За последние двадцать лет создано большое количество стандартов, посвященных управлению рисками ИБ: ISO/IEC 27005, NIST 800-30, РС БР ИББС-2.2-2009, COBIT Risk IT, BSI-Standard 100-3, MAGERIT, EBIOS, PCI DSS Risk Assessment Guidelines и прочие. Большой вклад в развитие теории рисков ИБ внесли научные группы и компании, разработавшие различные методики оценки рисков, такие как CRAMM, RiskWatch, OCTAVE, COBRA, ГРИФ, методика Microsoft.

Рассмотренные стандарты и методики отличаются используемыми шкалами оценки, перечнями угроз и уязвимостей, учитываемыми элементами риска, составом исходных данных. При этом оценка рисков в соответствии с ними осуществляется практически одинаково: собирается группа экспертов, определяющих значения элементов риска по некоторым качественным или количественным шкалам.

Еще одной особенностью, объединяющей существующие подходы к оценке рисков, является отождествление риска с угрозой или с комбинацией угрозы и уязвимости, что приводит к нескольким существенным недостаткам. Во-первых, угроза чаще всего является внешней по отношению к ИС, в результате чего трудно поддается исследованию и, как следствие, прогнозированию. Во-вторых, число возможных угроз зависит от степени детализации перечня, и может быть очень велико. При этом ни один из существующих перечней угроз нельзя назвать полным. В-третьих, различные угрозы могут приводить к схожим последствиям, вследствие чего полученные риски не будут обладать свойством аддитивности при расчете величины полного риска безопасности ИС. В-четвертых, рассмотренные подходы не позволяют однозначно определить причинно-следственные связи между идентифицированными рисками. Задача построения дерева событий упоминается в некоторых стандартах, однако инструменты для её быстрого и качественного решения без постоянного привлечения экспертов отсутствуют.

В работе 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 число типов компонентов ИС, невелико, что позволяет установить причинно-следственные связи между различными 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.

Модель состояний и переходов компонентов ИС. Множество компонентов ИС обозначается как $IS = \{O_1, O_2, ..., O_k\}$. Исходя из определения, а также анализа источников [0], [6], [7] можно выделить следующие типы компонентов ИС: информационные активы (ИА), программное обеспечение ПО), технические средства (ТС) и каналы связи (КС). Структурная диаграмма типов компонентов ИС представлена на рисунке 1.

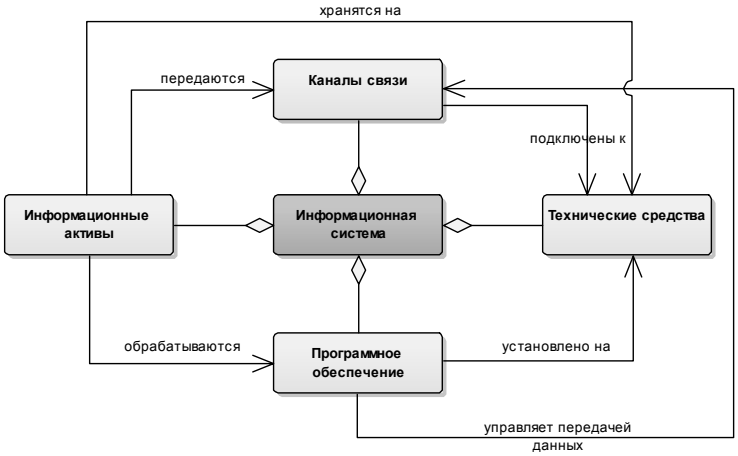


Рис.1. Структурная диаграмма типов компонентов ИС

ПО целесообразно разделять на системное и прикладное, поскольку защитные меры для общесистемного и прикладного уровней ИС могут различаться. В то же время это позволяет более детально рассмотреть граф последствий (атак). Следовательно, множество компонентов ИС можно также представить как:

$$IS = \{IA, ASW, SSW, HW, DC\}, \quad (2)$$

где IA – множество ИА, ASW – множество прикладного ПО; SSW – множество системного ПО; HW – множество ТС; DC – множество КС.

Каждый компонент ИС представлен в модели кортежем из пяти элементов:

$$O = [S, C, T, F_T, Q], \quad (3)$$

где

S – множество деструктивных состояний компонента ИС,

C – множество предпосылок (причин), приводящих к переходу;

T – множество переходов компонента ИС в деструктивные состояния S при возникновении причин *C*;

F_T – функция, определяющая вероятность перехода;

Q – множество последствий от переходов компонента ИС в деструктивные состояния.

Под деструктивным состоянием понимается нежелательное и незапланированное состояние компонента ИС, в котором он оказался в результате реализации одной или нескольких угроз. Объект, находящийся в деструктивном состоянии, обозначается как $O^{[S]}$, где вместо S указывается индекс одного или нескольких (через запятую) деструктивных состояний. Состояния компонентов ИС, отличные от деструктивных, считаются нормальными, а объект, находящийся в нормальном состоянии, обозначается как $O^{[N]}$. В ходе анализа различных методик моделирования угроз [0], оценки рисков [8], [9] и опроса специалистов в области ИБ были определены множества деструктивных состояний для каждого типа компонентов ИС:

а) информационный актив:
   - заблокирован (нарушена доступность), $IA^{[B]}$;
   - скомпрометирован (нарушена конфиденциальность), $IA^{[C]}$;
   - модифицирован (нарушена целостность), $IA^{[M]}$;

б) программное обеспечение:
   - заблокировано, $ASW^{[B]}/SSW^{[B]}$;
   - взломано, $ASW^{[H]}/SSW^{[H]}$;
   - модифицировано, $ASW^{[M]}/SSW^{[M]}$;

в) техническое средство:
   - заблокировано, $HW^{[B]}$;
   - повреждено, $HW^{[D]}$;
   - утеряно, $HW^{[L]}$;

– модифицировано, $HW^{[M]}$;

г) канал связи:

– поврежден, $DC^{[D]}$;

– взломан, $DC^{[H]}$.

Деструктивные состояния, предложенные в работе, не являются взаимоисключающими. Например, ТС может быть повреждено и утеряно: $HW^{[D,L]}$.

Под переходом понимается изменение состояния компонента информационной системы с нормального на деструктивное в результате реализации угрозы:

$$T_{ij}(O): O^{[N]} \rightarrow O^{[S_i]}, \quad (4)$$

где $T_{ij}(O)$ – функция перехода объекта O в деструктивное состояние S_i в результате возникновения j - ой предпосылки.

Обратные переходы, приводящие к изменению состояния компонента ИС с деструктивного на нормальное, возможны в результате реализации корректирующих защитных мер или при устранении причины перехода.

Предпосылками для перехода компонента ИС в деструктивное состояние могут быть:

– действия, предпринимаемые антропогенными источниками угроз, либо события, вызванные естественными источниками угроз;

– переход связанного компонента ИС в деструктивное состояние.

Сценарием реализации угроз называется один или несколько связанных переходов компонентов ИС в деструктивные состояния, вызванные действиями или событиями, происходящими от одного источника угроз. Некоторые из возможных сценариев реализации угроз, приводящих к нарушению доступности ИА, представлены на рисунке 2.

Первый переход в сценарии всегда обусловлен действиями источника угроз, под которым понимается субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации [0]. В большинстве стандартов, руководств и методических материалов выделяют естественные и искусственные (антропогенные) источники угроз [8]. Естественные источники угроз подразделяются на природные и техногенные, а антропогенные – на преднамеренных и непреднамеренных нарушителей.

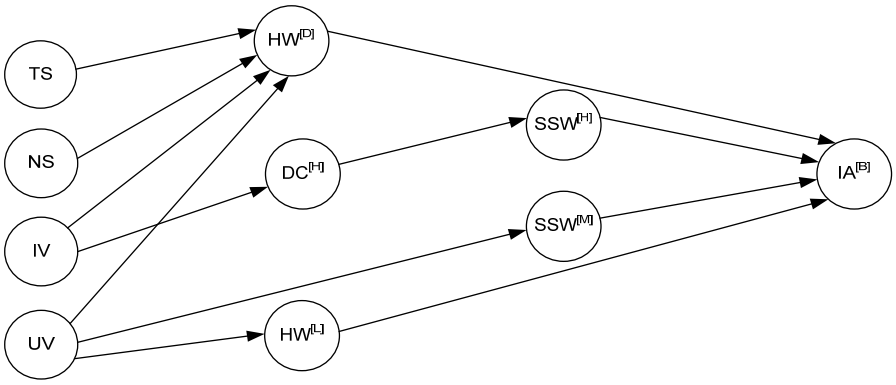


Рис.2. Сценарии реализации угроз, приводящих к нарушению конфиденциальности ИА

Множество источников угроз обозначается как:

$$ST = \{NS, TS, UV, IV\}, \quad (5)$$

где

ST – множество источников угроз,

NS – множество природных источников угроз;

TS – множество техногенных источников угроз;

UV – множество непреднамеренных нарушителей;

IV – множество преднамеренных нарушителей.

Для естественных и для антропогенных источников угроз определяется степень опасности D_{ST}, принимающая значения в интервале [0,1]. Степень опасности естественных источников угроз определяется на основании имеющихся статистических данных, либо методом экспертных оценок. Степень опасности антропогенных источников угроз определяется на основании модели нарушителя. Вопрос оценки степени опасности источников угроз выносится за рамки данной статьи.

Последующие (связанные) переходы сценария могут быть вызваны как дополнительными действиями данного источника, так и уже свершившимися переходами связанных компонентов ИС в

деструктивные состояния. Во избежание петель в модели определены направления причинно-следственных связей переходов для типов компонентов ИС. При физическом доступе сценарий реализации угроз для ИА может быть представлен как:

$$ST \to T(HW) \to T(SSW) \to T(ASW) \to T(IA). \quad (6)$$

Соответственно, при удалённом (логическом) доступе сценарий реализации угроз для ИА может быть представлен как:

$$ST \to T(DC) \to T(SSW) \to T(ASW) \to T(IA). \quad (7)$$

При этом в сценариях реализации угроз могут отсутствовать некоторые элементы из представленных в (6) и (7). Например, потеря ТС может привести к нарушению конфиденциальности, хранящего на нём ИА, без воздействия на ПО.

Для учета причинно-следственных связей между предпосылками и переходами формируются матрицы состояний и переходов для каждого компонента ИС. При формировании матрицы состояний и переходов из всего множества схожих предпосылок выбирается одна, вероятность возникновения которой наибольшая. То есть из всего множества преднамеренных нарушителей IV выбирается нарушитель, обладающий наибольшей степенью опасности. Это позволяет существенно упростить модель и не сказывается на результатах оценки.

Для каждого деструктивного состояния определяется функция вероятности перехода при возникновении предпосылки F_{Tij}, 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.

Для определения величины последствий от перехода компонента ИС в деструктивное состояние S_i для каждого типа компонентов ИС формируется классификатор последствий. При повреждении ТС и КС учитываются затраты на их восстановление и/или замену. При утере ТС учитываются затраты на его замену. Для остальных деструктивных состояний ПО, ТС и КС учитываются затраты на восстановительные работы по возвращению компонента ИС в нормальное состояние. Последствия от нарушения конфиденциальности, целостности и доступности информационного актива определяются исходя из высокоуровневых рисков для бизнес-функций, связанных с данным активом, которые могут быть обусловлены возникновением финансовых, репутационных, производственных, экологических, правовых и иных последствий.

Вопросы определения F_{Tij} и $Q_{[Si]}$ являются достаточно объёмными и выносятся за рамки данной статьи.

Для анализа всех возможных сценариев (путей) реализации угроз и нахождения наиболее вероятного из них строится граф последствий: $G_Q = \{V, H\}$. Граф G_Q является ориентированным и не содержит петель. Множество вершин графа обозначается как $G_Q : V = \{V_O, ST, S\}$. Помимо множества источников угроз ST и множества деструктивных состояний компонентов в графе вводится также фиктивная начальная вершина V_O. Множество рёбер графа $G : H = \{H_S, H_T\}$ содержит два подмножества:

- подмножество направленных рёбер H_S, соединяющих фиктивную вершину V_O со всеми вершинами подмножества источников угроз ST;
- подмножество направленных рёбер H_T, соответствующих переходам в матрице состояний и переходов и соединяющих вершины-предпосылки с вершинами-состояниями.

Вес ребра h_{ij} обозначается как I_{ij} и принимает значения в интервале (0;1]. Веса рёбер определяются согласно следующим выражениям:

$$\begin{cases} l_{ij} = -\ln(D_{STj}), \forall h_{ij} \in H_S \\ l_{ij} = -\ln(F_{Tij}), \forall h_{ij} \in H_T, \end{cases} \quad (8)$$

Благодаря данным преобразованиям задача нахождения наиболее возможного сценария, приводящего к переходу компонента ИС в деструктивное состояние сводится к задаче нахождения минимального пути в графе G_S. Для нахождения кратчайших путей L_i из вершины V_O во все

остальные вершины G_S существуют различные алгоритмы. Одним из самых известных и применяемых на практике является алгоритм Дейкстры, согласно которому кратчайший путь должен удовлетворять следующим условиям [3]:

$$\begin{cases} L_i = \sum_{i,j=0}^{n} l_{ij} \cdot \chi_{ij} \to \min \\ \sum_j \chi_{0j} = 1, \sum_j \chi_{jn} = 1 \,, \\ \sum_i \chi_{ki} = \sum_{j=0}^{n} \chi_{jk}, \overline{1, n-1} \end{cases} \quad (9)$$

где χ_{jn} = 1, если дуга (i, j) входит в путь L, χ_{jn} = 0, если дуга (i, j) не входит в путь L.

Вероятность перехода компонента ИС в деструктивное состояние определяется по формуле:

$$P_{[Si]} = \exp^{-L_i} . \quad (10)$$

Риск для k -го компонента ИС равен:

$$R_k = \sum_{i=1}^{I} P_{[Si]} \cdot Q_{[Si]} . \quad (11)$$

Полный риск для ИС равен сумме рисков для всех компонентов:

$$R_{FULL} = \sum_{k=1}^{K} R_k . \quad (12)$$

По результатам оценки рисков безопасности ИС осуществляется выбор защитных мер на основании показателя рискоёмкости активов [4].

Заключение и выводы. Представленная модель оценки рисков безопасности ИС на основе состояний и переходов позволяет осуществлять динамическую 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. Дальнейшие исследования направлены на доработку базовой модели оценки и разработку алгоритма её обучения на основе статистики инцидентов ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК 15.02.2008).
2. Вихров Н.М., Нырков А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С., Нурдинов Р.А.. Анализ информационных рисков // Морской вестник. 2015. № 3. С.81
3. Бурков В.Н., Заложнев А.Ю., Новиков Д.А. Теория графов в управлении организационными системами. М.: Синтег, 2001.- 124 с.
4. Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации // Современные проблемы науки и образования. – 2013. – № 2; URL: http://www.science-education.ru/108-9131.
5. Петров В. Н. Информационные системы – СПб.: Питер, 2003. – 688 с: ил. ISBN 5-318-00561-6
6. Федеральный закон РФ № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» (ред. от 28.07.2012).
7. Федеральный закон РФ № 152-ФЗ от 27.07.2006 «О персональных данных».
8. ISO/IEC 27005:2011 Информационные технологии – Методы и средства обеспечения безопасности.
9. NIST SP 800-30 Risk Management Guide for Information Technology Systems, 2012, 95 с.

УДК 004.056

ИЗГИБ ОПТИЧЕСКОГО ВОЛОКНА КАК ОДИН ИЗ СПОСОБОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Петрук Татьяна Николаевна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
e-mail: tatiana.curt@gmail.com

Аннотация. В статье детально рассмотрен один из способов создания канала утечки информации. Данный способ основан на принципе распространения света через волокно посредством полного внутреннего отражения. Для точной оценки потерь при сгибании оптоволокна был проведен эксперимент, который наглядно показывает возможность получения оптического сигнала с волокна.

Ключевые слова: *оптическое волокно; утечка информации.*

BENDING THE OPTICAL FIBER AS ONE OF THE WAYS OF GETTING INFORMATION

Petruk Tatiana,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: tatiana.curt@gmail.com

Abstract: The article reviewed in detail the one of the ways to create a channel of information leakage.This method is based on the principle of light propagation through the fiber by total internal reflection.For an accurate assessment of losses by bending the fiber was an experiment that demonstrates the possibility of obtaining the optical signal from the fiber.

Keywords: *an optical fiber; information leak.*

Введение. 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.

Однако, после проведения некоторых исследований, стало очевидно, что съем информации в ВОЛС возможен, хотя достаточно сложен с технической стороны, нежели в случае с иными линиями связи. Причина тому физические принципы распространения электромагнитной волны в световоде.

Таким образом, поставленная задача заключается в глубоком анализе возможных каналов утечки информации (КУИ), изучении и предложении способов защиты.

Один из способов создания КУИ подразумевает под собой разрыв кабеля и отвод мощности при помощи специальной аппаратуры [1].

Это действительно позволит осуществить несанкционированный доступ (НСД), но такие способы являются совершенно не опасными.

Во-первых, реализация их на практике сопряжена с рядом трудностей, а также выполнение выреза очень сложно выполнить в короткий срок и остаться незамеченным.

Во-вторых, существует множество мер обнаружения и противодействия данным способам, которые разработаны давно и действуют эффективно. Что нельзя с уверенностью утверждать в остальных возможных случаях.

Второй способ заключается в отводе оптической мощности без нарушения целостности кабеля. Один из таких методов, на который стоит обратить внимание, это изгиб волокна.

Для более глубокого изучения отвода мощности и потерь на изгибе оптического волокна (ОВ) в лабораторных условиях был проведен эксперимент.

Экспериментальная установка представлена на рисунке 1.

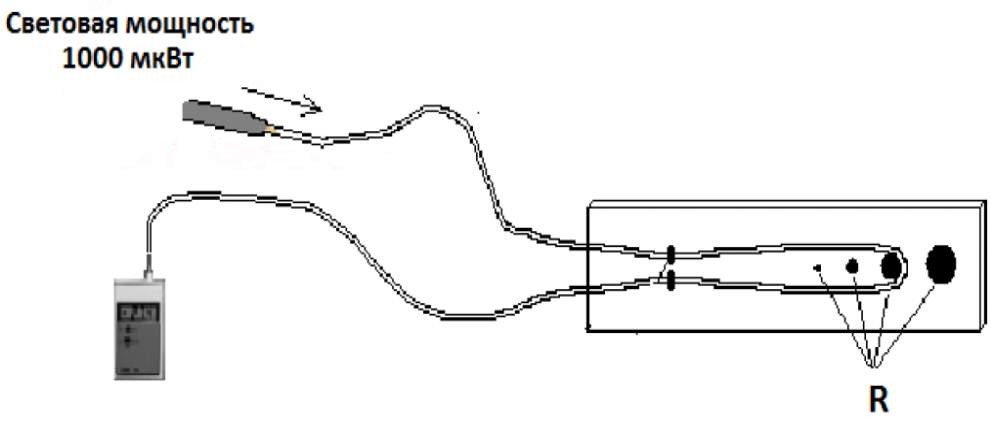


Рис. 1. Схема экспериментальной установки

Для контроля выходящей мощности был использован измеритель мощности. Середина волокна была закреплена на специально подготовленный штатив, на котором закреплялись эталоны радиусов.

Измерение значения мощности проводилось два раза: сначала до изгиба, и когда волокно было изогнуто.

После обработки этих данных было найдено среднее относительное значение потерь для каждого из радиусов и построен график зависимости (Рис.2).

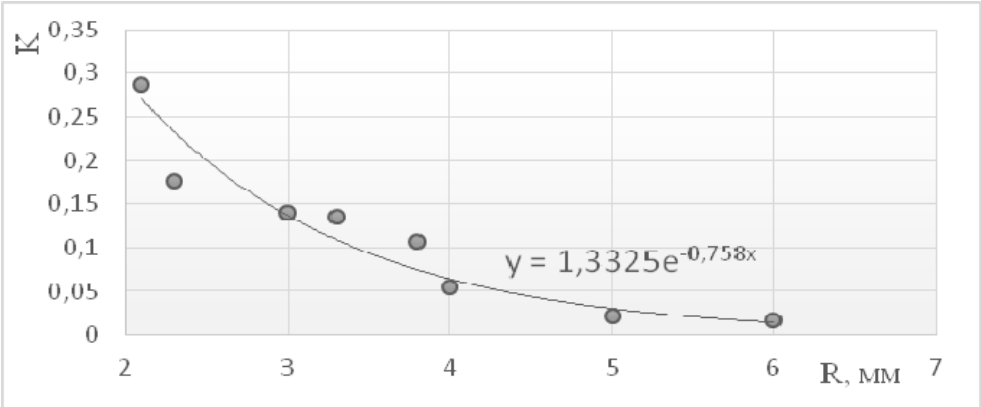


Рис.2.Экспериментальная зависимость потерь от радиуса изгиба

Так же можно получить и аналитическое выражение для аппроксимирующей зависимости, которым можно будет пользоваться для нахождения оптимального радиуса изгиба:

$$K = 1{,}3325e^{-0{,}758R}. \quad (1)$$

Существует специальное устройство подключения на изгибе волокна – ответвитель-прищепка. Устройство обеспечивает двунаправленное подключение к одномодовому волокну без его разрыва. При подключении прищепки образуется изгиб и в результате некоторая часть излучения покидает светопроводящую сердцевину и выходит наружу. Регулируя радиус изгиба можно добиться как полного выхода, так и частичного входа излучения.

В связи с наличием потенциальной угрозы несанкционированного съёма информации во всем мире ведутся работы по защите ВОЛС.

Большинство средств защиты построены так, чтобы затруднить механическую разделку кабеля и воспрепятствовать доступу к ОВ, или связанны с разработкой различных устройств контроля параметров оптических сигналов на выходе ОВ, например, метод импульсной рефлектометрии. Однако, ни один нельзя считать достаточно эффективным и надёжным говоря об НСД на изгибе ОВ. Существующие криптографические методы являются более эффективными, но в ходе преобразований уменьшают пропускную способность, а это одно из главных достоинств ВОЛС.

Заключение. На основе проведенного анализа КУИ, изучения конкретных способов защиты, доказательства уязвимости ОВ на практике, вопрос о защищенности ВОЛС требует пересмотра. В связи с возможностью компрометации передаваемых данных или их модификации нельзя обойтись без разработки методов защиты на основе квантовой криптографии.

Такие методы потенциально обеспечивают высокую степень защиты от перехвата информации на линии связи за счет передачи данных в виде отдельных фотонов, поскольку неразрушающее измерение их квантовых состояний в канале связи перехватчиком невозможно, а факт перехвата фотонов из канала может быть выявлен по изменению вероятностных характеристик последовательности фотонов.

Таким образом, квантовая криптография является перспективным направлением для защиты информации в ВОЛС.

Согласно данным на 2015 год Минпромторг принял решение включить в программу импортозамещения оптоволокно и в таком случае, Саранское производство должно стать первым в России предприятием, выпускающим оптическое волокно.

Не менее важной проблемой в области защиты ВОЛС, на мой взгляд, является разработка нормативной и методической базы и документов, обеспечивающих и регламентирующих как разработку защищенных ВОЛС, так и порядок их внедрения в сетях связи.

Это поможет исключить заблуждения, которые прослеживаются как в повседневной жизни, так и в Российских нормативных документах.

СПИСОК ЛИТЕРАТУРЫ

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами // С-Петербург: НИУ ИТМО, 2013. 416 с.
2. Румянцев К.Е., Хайров И.Е. Передача конфиденциальной информации по волоконно-оптическим линиям связи, защищенная от несанкционированного доступа, – Научн.-практ. журн., № 1, 2003 – С. 72–79.
3. Статья из интернет-журнала: «Скрытное подсоедините к оптоволокну: методы и предосторожности», 2014. [Электронный ресурс] — URL: http://habrahabr.ru/post/176677/ режим доступа: свободный (дата обращения: 01.05.15).
4. Спирин А.А. Введение в технику волоконно-оптических сетей. [Электронный ресурс] — URL: http://www.citforum.ru/nets/optic/optic1.shtml режим доступа: свободный (дата обращения: 29.04.15).

УДК 004.056

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРИМЕТРА АВТОМАТИЗИРОВАННЫХ КАРТОГРАФИЧЕСКИХ СИСТЕМ

Солодянников Александр Владимирович, Пилипов Михаил Васильевич,
Парамонов Андрей Владимирович,
ЗАО «Ассоциация специалистов информационных систем» (ЗАО «АСИС»),
Россия, Санкт-Петербург, ул. Кантемировская, д. 7,
e-mail: info@spbissa.ru

Аннотация: В статье рассмотрены способы, технические и программные средства, применяемые для защиты периметра автоматизированных картографических систем.

Ключевые слова: *Информационная безопасность, автоматизированные картографические системы.*

PERIMETER PROTECTION IN AUTOMATED MAPPING SYSTEMS

Solodyannikov Alexander, Pilipov Mikhail, Paramonov Andrey
JSC «Associaci» (JSC «ASIS»),
Russia, St. Petersburg, ul. Kantemirovskaya, 7,
e-mail: info@spbissa.ru

Abstract: The article discusses ways hardware and software used to protect the perimeter of automated mapping systems.

Keywords: *IT security, automated mapping systems.*

Введение. Развитие вычислительной техники, программных средств и телекоммуникационных систем, повлекло за собой широкое применение этих технологий в картографическом деле.

В общем случае картографическая информация представляет собой данные с различным уровнем конфиденциальности – от общедоступной до сведений, составляющих государственную тайну. При обработке в картографических системах одной из задач является защита информации, целью которой является предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации [1].

Характеристиками 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 (СОП);

– применение в качестве банка исходных данных единой системы геопространственной информации (открытой и закрытой);

– наличие как отечественных конечных потребителей картографической продукции (органы государственной и исполнительной власти, юридические и физические лица), так и зарубежных;

– 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 отчуждаемых физических носителей 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:

1). Необходимость подключения АКС к сетям общего пользования;

2). Необходимость контроля двунаправленного потока информации (извне и в систему) по всем физическим каналам, имеющим выход за пределы контролируемой зоны;

3). Необходимость применения организационных и технических мер защиты информации, исключающих неправомерное применение отчуждаемых физических носителей информации.

Способами реализации мероприятий по защите периметра, для потоков информации, передаваемой в АКС (в первую очередь, из СОП), является применение в системе защиты АКС:

– межсетевых экранов;
– систем обнаружения/предотвращения вторжений (IPS/IDS- системы);
– систем защиты от НСД к информации;
– средств антивирусной защиты;

Для потоков информации, передаваемой из АКС за ее периметр (в первую очередь, в СОП), способами реализации мероприятий по защите периметра является применение:

– межсетевых экранов;
– прокси-серверов;
– систем защиты от НСД к информации;
– систем предотвращения утечки информации с ограниченным доступом (DLP- системы) [2].

Необходимость применения тех или иных средств и систем для защиты периметра должна определяться в каждом конкретном случае, так как одни и те же функции защиты информации могут реализовываться различными средствами, например, контроль применения отчуждаемых физических носителей информации может выполняться системами защиты от НСД и DLP- системами.

Для определения полноты выполненных мероприятий по защите периметра системы необходимо провести контроль эффективности. В настоящее время, в качестве средств контроля (анализа) защищенности (в том числе сертифицированных ФСТЭК России) применяются сетевые сканеры, базирующиеся на зарубежных программных продуктах.

Действующие нормативно-методические документы (НМД) для проведения контроля эффективности проведенных мероприятий по защите периметра не в полной мере отвечают специфике защиты информации в АКС, так как не позволяют оценить:

– эффективность защиты периметра АКС в целом, с учетом всех средств и систем информационной безопасности;

– достаточность мероприятий по защите информации для исходящих из АКС потоков информации.

Одной из проблем, возникающих при организации контроля эффективности защиты периметра, является отсутствие конкретных требований к тестовым воздействиям на периметр системы, имитирующим действия злоумышленников и легальных пользователей, находящихся как снаружи периметра, так и внутри его. Это, в свою очередь, может привести к снижению качества системы защиты информации в целом.

Для решения этих задач в ЗАО «АСИС» выполнены следующие работы:

– на основе государственных стандартов информационной безопасности серии ГОСТ Р 15408 разработаны модели элементов периметра АКС как объектов оценки, цели безопасности и политики безопасности, сформирован перечень требований к объекту оценки и среде функционирования, которые позволяют компенсировать недостаточную полноту существующих НМД;

– разработаны требования к тестовым воздействиям на периметр системы, имитирующим действия злоумышленников и легальных пользователей, как снаружи периметра, так и внутри его.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51624-2000 Автоматизированные системы в защищенном исполнении. Общие положения.
2. Обзор DLP-систем на мировом и российском рынке (электронный ресурс). http://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014 (дата обращения 29.09.2015).

УДК 004.056.53

ОПТИЧЕСКОЕ ТУННЕЛИРОВАНИЕ КАК МЕТОД ФОРМИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

Ральникова Наталья Сергеевна,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, д.49.,
e-mail: natalya.ralnikova@gmail.com

Аннотация: В данной статье рассказывается о существовании методов формирования каналов утечки информации, передаваемой по волоконно-оптическим линиям связи, при подключении без

нарушения целостности, и подробно рассматривается наиболее скрытный из них – оптическое туннелирование.

Ключевые слова: *оптоволокно; каналы утечки; нарушение полного внутреннего отражения; оптическое туннелирование.*

OPTICAL TUNNELING AS A METHOD OF FORMING A CHANNELS OF INFORMATION LEAKEGE, TRANSMITTED ON FIBER-OPTICAL COMMUNICATION LINES

Natalya Ralnikova,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mail: natalya.ralnikova@gmail.com

Abstract: This article discusses the existence of methods for forming channel leakage of information transmitted on the fiber-optic line, when connected without damaging the integrity and considers in details the method optical tunneling as the most secretive of them.

Keywords: *Fiber-optic; leakage channels; frustrated total internal reflection; optical tunneling.*

Введение. 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. ВОЛС применяются как в больших магистральных линиях передачи, так и в локальных компьютерных сетях. Свое широкое распространение оптоволокно получило благодаря ряду преимуществ над другими каналами связи, к которым можно отнести широкую полосу пропускания, высокую частоту несущей, низкий уровень шумов, высокую помехозащищенность, высокую защищенность от несанкционированного доступа [1].

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 и сигнал, передаваемый по ВОЛС, не требует защиты. 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 (рисунок 1) [2].

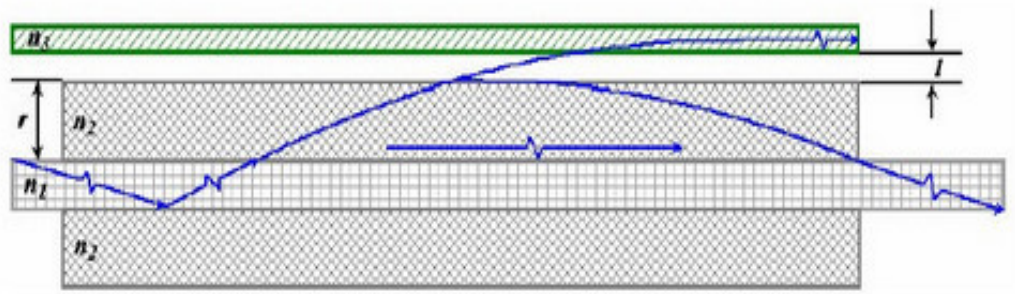


Рис. 1. Формирование канала утечки оптическим туннелированием.
n1 и n2 – показатели преломления сердцевины и оболочки оптоволокна,
n3 – показатель преломления дополнительного оптоволокна

При распространении света в оптическом волокне часть светового потока выходит за пределы сердцевины оптоволокна. Интенсивность I излучения вышедшего из сердцевины в оболочку оптоволокна на расстояние r в зависимости от угла падения на границе сердцевина-оболочка φ определяется выражением:

$$I = I_0 \exp(-4\pi n_1 \left(\frac{r}{\lambda}\right) \sqrt{\sin^2 \varphi - \sin^2 \varphi_r}), \quad (1)$$

где

I_0 – интенсивность падающего излучения,

φ – угол падения.

φ_r – угол полного отражения.

При приближении угла падения φ к углу полного отражения φ_r 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.

Интенсивность излучения переходящего в дополнительный волновод определяется выражением:

$$I = I_0 \sin^2(kS), \quad (2)$$

где

k – коэффициент связи оптических волокон,

S – длина оптического контакта двух волокон.

Максимум значения коэффициента связи достигается при нулевом расстоянии между оболочкой и дополнительным оптоволокном $(I = 0)$ и показателе преломления дополнительного волокна $n3 = n1$. Как видно из выражения, излучение из основного оптического волновода переходит в дополнительный волновод полностью при некотором значении длины оптического контакта $S = \pi / 2k$. При дальнейшем увеличении длины оптического контакта происходит обратный процесс. Таким образом, излучение периодически переходит из одного волновода в другой, если не учитывать потери на поглощение, рассеяние [2].

Сформировать канал утечки данным способом из волокна в специальное волокно можно при помощи специального оптического соединителя, работающего на принципе оптического туннелирования. Структурная съема такого оптического соединителя представлена на рисунке 2 [3].

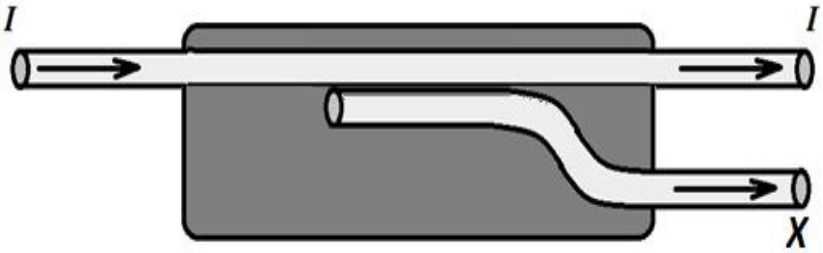


Рис. 2. Структурная схема оптического соединителя, работающего на принципе оптического туннелирования

Примером такого оптического соединителя может служить механический соединитель оптических волокон Fibrlok II 2539. Его изображение представлено на рисунке 3.

Рис. 3. 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.

Заключение. 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.

СПИСОК ЛИТЕРАТУРЫ

1. Ральникова Н.С. Каналы утечки информации в волоконно-оптических линиях связи // V Межвузовская научно-практическая конференция аспирантов, студентов и курсантов «Современные тенденции и перспективы развития водного транспорта России» 14 мая 2014 года –2014, С. 311–315.
2. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения // Информационное противодействие угрозам терроризма. – 2005. № 4, С.194–204
3. Гришачев В.В. Учебное пособие «Информационная безопасность волоконно-оптических технологий». Часть II [Электронный ресурс]. – Режим доступа: http://analitika.info/public/files/grishachev-lectures_isfot_part_2.pdf, свободный. – Загл. с экрана. – Яз. рус.

УДК 004.93’1

МОДЕЛИ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ ЭНТРОПИЙНЫХ ХАРАКТЕРИСТИК

Сорокин Иван Витальевич[1], Копыльцов Александр Васильевич[2],
[1]ООО «Доктор Веб»,
Россия, Санкт-Петербург,
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
e-mails: sorokin.ivan@mail.ru, kopyl2001@mail.ru.

Аннотация: В статье рассмотрена модель распознавания вредоносных программ, включающая в себя использование вейвлет-анализа для сегментации файлов на сегменты с разной энтропией и редакционного расстояния между последовательностями сегментов для определения близости файлов.

Ключевые слова: *энтропия; вейвлет анализ; редакционное расстояние; вредоносные программы*

MODEL OF MALWARE RECOGNITION BASED ON ENTROPY FEATURES

Sorokin Ivan Vital'evich[1], Kopyltsov Alexander Vasilevich[2],
[1] "Doctor Web", Ltd,
Russia, St. Petersburg,
[2]The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
e-mails: sorokin.ivan@mail.ru, kopyl2001@mail.ru.

Abstract*:* The article describes a model of malware recognition, which consists of using wavelet analysis for the segmentation of files into segments of different entropy levels and using edit distance between sequence segments to determine the similarity of the files.

Keywords: *entropy; wavelet analysis; edit distance; malware*

В настоящее время имеется большое количество различных вредоносных программ. Для их обезвреживания разработаны различные подходы. Среди всего многообразия угроз в последние годы существенно увеличилось количество вредоносных программ, в которых используются методы упаковки и запутывания программного кода. Применение известных методов обезвреживания не позволяет эффективно бороться с такими вредоносными программами. Поэтому актуальным является разработка новых моделей, методов и средств выявления подобных угроз [1 – 4]. Целью работы является повышение качества выявления упакованных вредоносных программ за счет создания новых математических моделей и алгоритмов распознавания, позволяющих уменьшить вычислительные ресурсы антивирусного программного обеспечения. Рассматривается система распознавания упакованных вредоносных программ, состоящая из двух основных частей: модуль сегментации файлов и модуль сравнения файлов. В первом модуле осуществляется предварительная обработка и вейвлет-анализ входных файлов. Во втором модуле сравниваются

сегментированные файлы между собой с использованием одного из двух подходов либо на основе векторной модели, либо на основе использования взвешенного расстояния редактирования.

Далее эти модули рассмотрены более подробно. Рассматривается модуль сегментации входных файлов. Сначала рассматривается алгоритм предварительной обработки файла, а затем вейвлет-анализ и сегментация файла. Этап предварительной обработки заключается в использовании метода скользящего окна, позволяющего представить содержимое файла в виде ряда (рисунок 1). Подсчет энтропии в i-м окне осуществляется с учетом частоты появления различных байтов по следующей формуле:

$$y_i = -\sum_{j=1}^{m} p(j)\log_2 p(j), \tag{1}$$

где $p(j)$ – частота появления j-го байта в i-м окне, n – количество различных байтов в окне.

Этап вейвлет-анализа является основным в этом модуле и служит для разбиения ряда на сегменты, обладающие однородной структурой. Для этого предлагается использование дискретного избыточного варианта вейвлет-преобразования, вычисляемого по формуле:

$$W(a,b) = a^{-0,5}\sum_{i=a}^{b+a} y_i \psi_{HAAR}\left(\frac{i-b}{a}\right), \tag{2}$$

где a – параметр масштаба, b – параметр сдвига, y_1 – информационная энтропия в i-м окне. В качестве базисного вейвлета используется вейвлет Хаара *HAAR*, обладающий несимметричной формой и нулевым моментом равным нулю. Изменение параметра сдвига b осуществляется последовательно от 1 до N. Это приводит к избыточности вычислений, которая позволяет решать проблему инвариантности при сдвиге исходных данных. Параметр масштаба a изменяется, как 2 в степени от 1 до 5, т.е. 2,4,8,16,32. Благодаря этому появляется возможность на каждом следующем масштабе преобразования использовать значения коэффициентов, вычисленные на предыдущем шаге. Вейвлет коэффициенты $W(a,b)$ используются для анализа и сегментации анализируемого ряда. Суть алгоритма сегментации заключается в поиске значений локальных экстремумов на каждом шаге преобразования. Границы итоговых сегментов определяются найденными локальными экстремумами. В итоге, на выходе модуля сегментации файлов получается последовательность сегментов, каждый из которых характеризуется определенной длиной (количеством байтов). Дальнейшее использование характеристик сегментов зависит от выбранной модели сравнения: либо векторной модели, либо модели основанной на расстоянии редактирования Левенштейна.

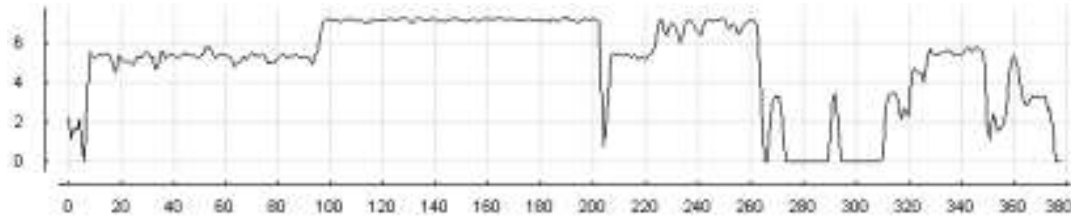


Рис. 1. Энтропия файла (по оси абсцисс – номера окон в файле, по оси ординат – информационная энтропия в окне)

Для сравнения вредоносных программ описывается векторная модель, при которой каждый компонент вектора обозначает характерный сегмент или набор сегментов файла. Для того чтобы использовать такую векторную модель необходимо решить вопрос определения всех возможных сегментов, которые могут встречаться в файлах упакованных вредоносных программ. Для уменьшения общего количества сегментов предлагается выявлять похожие сегменты в разных файлах и выделять их в одну группу.

В качестве критериев для выявления похожих сегментов предлагается использовать один из трех подходов, которые учитывают: либо размер и энтропию сегмента, либо частоту появления различных байтов в сегменте, либо нейросетевую модель.

Из трех перечисленных подходов, наиболее трудоемким является последний подход, предполагающий использование нейронной сети неокогнитрон. В этом подходе на вход сети подается изображение, интенсивность окраски точек которого определяется значением (от 0 до 255) байтов в сегменте. Нейронная сеть обучается таким образом, чтобы осуществлялось запоминание взаимного расположения байтов в отдельном сегменте.

Предлагается модель сравнения файлов, в которой файлы описываются последовательностью сегментов, а близость файлов между собой определяется с использованием взвешенного расстояния редактирования, основанного на метрике Левенштейна. Ключевым моментом в предлагаемом подходе является функция стоимости g, которая определяет величину штрафа за несовпадение двух сегментов,

каждый из которых характеризуется двумя величинами (размером и энтропией). Обозначим размеры (количество байтов) двух сегментов через l_1 и l_2, а соответствующие значения энтропии – через h_1 и h_2. Тогда общий штраф между двумя сегментами вычисляется следующим образом:

$$g = \alpha \frac{|l_1 - l_2|}{l_1 + l_2} + (1-\alpha)\left(\frac{1}{1+\exp(\beta|h_1 - h_2| + \gamma)} - \delta \right), \quad (3)$$

где первое слагаемое обозначает штраф за разницу в размерах, а второе – за разницу в энтропии двух сегментов, $\alpha, \beta, \gamma, \delta$ – коэффициенты. Для сравнения двух вредоносных программ, с учетом выражения (3) для функции стоимости g, предлагается алгоритм, основанный на глобальном выравнивании последовательностей. Алгоритм заключается в заполнении двумерного массива C.

На каждом шаге заполнения массива C осуществляется одна из трех операций преобразования: замещение, удаление или вставка сегмента файла. Алгоритм позволяет определить общий штраф при сравнении последовательностей сегментов двух файлов и произвести их выравнивание, т.е. найти похожие сегменты в файлах. Также появляется возможность определить степень похожести двух файлов (выраженную в процентах), вычисляемую как доля фактического штрафа от максимально возможного штрафа за несовпадение двух файлов.

Рассматривается эффективность предложенных подходов для выявления упакованных вредоносных программ. Сначала оценивается количество операций при реализации предлагаемых алгоритмов, а затем приводятся результаты тестирования системы распознавания упакованных вредоносных программ. Для тестирования составлены выборки пяти различных семейств упакованных вредоносных программ (443 файла) и набор чистых (не вредоносных) программ (100 файлов). Под семейством подразумевается совокупность вредоносных программ, относящихся к одной из пяти угроз: Backdoor.Tdss (100 файлов), BackDoor.Maxplus (ZeroAccess) (63 файла), BackDoor.Butter (Mariposa) (100 файлов), Trojan.Mayachok (Cidox) (80 файлов), BackDoor.Slym (Kelihos) (100 файлов). Результаты тестирования показывают, что с помощью алгоритма, построенного на основе расстояния редактирования, можно отделять упакованные вредоносные программы от чистых программ и распознавать отдельные семейства вредоносных программ между собой.

Сравнение алгоритма, основанного на взвешенном расстоянии редактирования, с двумя другими подходами (сигнатурно-байтовый и модель поведения под эмулятором), используемыми в антивирусных программных продуктах ООО «Доктор Веб», показало, что при распознавании большинства тестовых файлов (373 из 443) предлагаемый алгоритм показывает лучшие характеристики.

Во-первых, лучше устойчивость к защитным методам обфускации и антиэмуляции, чем у детектирования по модели поведения.

Во-вторых, при отсутствии ошибок 1-го рода, нормированный уровень ошибок 2-го рода составил 15,8%, что меньше, чем у сигнатурного подхода (26,4%). Для сравнения подходов была создана база данных антивирусных записей, содержащая информацию о вредоносных программах. В качестве показателя качества использовалось минимальное количество записей необходимых для детектирования вредоносных программ. Такая эмпирическая оценка характеризует обобщающую способность распознавания. Чем меньше количество записей необходимых для тестовой выборки, тем больше вероятность обнаружить вредоносную программу, не вошедшую в тестовый набор.

В таблице 1 представлены результаты сравнения для детектирования 100 вредоносных программ Backdoor.Tdss.

Таблица 1

Результаты сравнения вредоносных программ Backdoor.Tdss

Способ обнаружения вредоносных программ	Количество файлов детектируемых одной из шести антивирусных записей						Итого записей
	1	**2**	**3**	**4**	**5**	**6**	
Сигнатурно-байтовый	9	9	12	13	28	29	6
Модель поведения	9	15	35	41			4
Энтропийный	50	50					2

Из результатов проведенного эксперимента видно, что предлагаемый подход для распознавания упакованных вредоносных программ, требует меньшее количество антивирусных записей, чем другие подходы. В некоторых случаях, предлагаемый подход позволяет существенно сократить объем антивирусной базы данных. Например, для детектирования 63 вредоносных программ BackDoor.Maxplus требуется 63 сигнатурных записи (защита от выявления по модели поведения), занимающих в базе 974 байта. При использовании предлагаемого подхода понадобится три энтропийные записи, которые займут 190 байтов. Уменьшение количества антивирусных записей уменьшает не только объем базы данных, но и время обработки проверяемых файлов. Все это подтверждает эффективность предлагаемого подхода для распознавания упакованных вредоносных программ.

Таким образом, разработан алгоритм сегментации файлов, основанный на вейвлет-анализе энтропийных характеристик файлов. Используемый способ вычисления коэффициентов вейвлет-преобразования позволяет проводить поиск границ итоговых сегментов при минимальных числовых расчетах.

Предложено три способа описания сегментов файлов. В первом случае учитывается размер (количество байтов) и энтропия сегмента файла. Во втором случае используется частота появления байтов в сегменте. В третьем – модель неокогнитрона, позволяющая запоминать расположение отдельных байтов внутри сегмента файла. Предложен подход по использованию векторной модели для представления и сравнения файлов между собой, в которой компоненты вектора определяются одним из трех способов описания сегментированных участков файлов. Разработан метод идентификации упакованных вредоносных программ, основанный на взвешенном расстоянии редактирования для последовательностей сегментов, характеризующиеся двумя значениями: размером и информационной энтропией.

СПИСОК ЛИТЕРАТУРЫ

1. Копыльцов А.В., Сорокин И.В. Вейвлет-анализ структурной энтропии файлов // Известия РГПУ им. А.И.Герцена. – 2011. – №138. – С.7–15.
2. Копыльцов А.В., Сорокин И.В. Алгоритм выравнивания последовательностей сегментов файлов // Вестник ИНЖЭКОНа, серия «Технические науки». – 2011. – №8(51), –С.31–37.
3. Сорокин И.В., Копыльцов А.В. Использование неокогнитрона для распознавания вредоносных файлов // Известия СПбГЭТУ «ЛЭТИ». – 2013. – №3. – С.45–51.
4. Sorokin I. Comparing files using structural entropy // Journal in computer virology. – 2011. – Vol. 7. – N4. – pp.259–265.

УДК 004.056.53, 004.896

ОТ КЛАССИЧЕСКИХ К МНОГОАГЕНТНЫМ СИСТЕМАМ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Федотова Алена Валериевна, Волков Андрей Валентинович, Тарасов Валерий Борисович,
Московский государственный технический университет им.Н.Э. Баумана,
Россия, Москва, ул. 2-я Бауманская, д. 5,
e-mails: afedotova.bmstu@gmail.com, a64v@yandex.ru, vbulbov@ yahoo.com

Аннотация: В статье представлен обзор, рассуждение и исследование в области развития многоагентных систем, занимающихся безопасностью данных. Проведено исследование возможных угроз и уязвимостей информационного контура машиностроительного предприятия, каналов потерь данных и тех типов документов, которые наиболее сильно подвержены атакам злоумышленников. Был проведен анализ подходов к созданию программного обеспечения, позволяющего с некоторой долей вероятности предотвратить потерю данных в корпоративной информационной системе предприятия. В результате проведенных исследований возможно сделать вывод, что многоагентные системы все больше проникают в область разработки программного обеспечения, однако сложность реализации интеллектуальных алгоритмов создает высокий порог по созданию таких систем.

Ключевые слова: *многоагентные системы; информационная безопасность; корпоративная информация.*

FROM THE CLASSICAL TO MULTI-AGENT SYSTEMS OF CORPORATE DATA PROTECTION

Alena V. Fedotova, Andrey V. Volkov, Valery B. Tarassov,
Bauman Moscow State Technical University,
Russia, Moscow, 2-ya Baumanskaya str., 5,
e-mails: afedotova.bmstu@gmail.com, a64v@yandex.ru, vbulbov@ yahoo.com

Abstract: The article presents research in the field of development of multi-agent data protection systems. The research of possible threats and vulnerabilities of the information loop machine-building enterprise, data loss channel and the types of documents that are most heavily exposed to malicious attacks was conducted. An analysis of approaches to the creation of software that allows a certain degree of probability to prevent data loss in the corporate information systems of the enterprise is presented. The studies may conclude that multi-agent systems are increasingly penetrate into the area of software development, but the complexity of the implementation of intelligent algorithms creates a higher threshold for the establishment of such systems.

Keywords: *Multi-agent System; Information Security; Corporate data.*

Введение. Для обеспечения базового уровня информационной безопасности корпоративной системы достаточно классифицировать обрабатываемую информацию, регламентировать процессы ее обработки, активировать и настроить встроенные механизмы защиты информации, а также вовремя применять обновления безопасности. Однако на практике с этим возникает ряд проблем [1].

Уязвимости корпоративных информационных систем. Регламенты обработки конфиденциальной информации, разработанные специалистами из области информационной безопасности, могут быть плохо совместимы с архитектурой системы. При этом технические

специалисты обычно относятся к таким регламентам отрицательно, так как они ограничивают полномочия пользователей и администраторов, вводят зачастую громоздкие процедуры согласования и разрешения, могут требовать множества доработок.

Пренебрежение государственными стандартами и регламентами может вести к появлению в информационной системе ряда опасных уязвимостей, позволяющих злоумышленникам использовать информацию, которую хранит информационная система.

Если обратиться к статистике, то можно сказать, что сложность проведения атак в 2014 году оказалась заметно ниже, чем в предыдущие годы, а преодолеть сетевой периметр в 60% систем оказалось возможно через уязвимости веб-приложений [6].

Также в 2014 году существенно снизился уровень осведомленности сотрудников компаний по вопросам безопасности: они стали во много раз чаще переходить по незнакомым ссылкам и открывать приложенные к письмам файлы. Такие наблюдения содержатся в исследовании компании Positive Technologies на основе тестов на проникновение, проводившихся в 2014 году, и сравнения полученных данных с прошлогодними результатами.

Приведем примеры наиболее распространенных уязвимостей в современных корпоративных информационных системах:

- интерфейсы управления оборудованием;
- словарные пароли;
- использование открытых протоколов передачи данных;
- недостатки конфигурации SSL;
- уязвимые версии ПО;
- SQL-инъекции;
- интерфейсы доступа к СУБД;
- открытая документация к веб-сервисам приложений;
- наличие интерфейса загрузки файлов;
- хранение важных данных в открытом виде;

Приведен список наиболее распространенных групп уязвимостей, с которыми сталкиваются корпоративные информационные системы.

Современная система защиты корпоративной информации. Для того чтобы защитить любую информационную систему, необходимо перекрыть периметр уязвимостей, что сделать полностью не представляется никакой возможности. Однако перекрывать весь периметр нет никакой необходимости, поскольку необходимо снизить вероятности успешных атак на активы предприятия [1], [7].

Система защиты информации строятся исходя из этих принципов и в своем составе может иметь следующие компоненты и комплекс мер по защите информационной системы:

- системы защиты локальных вычислительных сетей (межсетевые экраны);
- системы шифрования документации;
- системы предотвращения потери данных;
- системы безопасного хранения и сбора паролей;
- программное обеспечение, использующее нестандартные протоколы передачи информации;
- сегментированную локальную вычислительную сеть.

Вышеприведенные компоненты и меры позволяют закрыть большинство уязвимостей информационных систем.

Создание программного обеспечения систем защиты информации. Как было приведено выше программное обеспечение в корпоративной защите информации играет немалую роль. Компоненты системы защиты информации могут быть и аппаратными, однако рассмотрим программную их составляющую:

- системы шифрования документации;
- системы предотвращения потери данных;
- системы безопасного хранения и сбора паролей.

Для реализации систем шифрования документации, небоходимо использовать стандартные, проверенные временем алгоритмы шифрования, такие как: AES, ГОСТ 28147-89, DES, RC2, RC5. Затем разработать программу реализующую шифрование документов, одним из способов [9].

Для систем безопасного хранения и сбора паролей, необходимо использовать криптографические хэш-функции, обеспечивающие отображение реальных паролей в иные последовательности символов. Передавать хэши в централизованное хранилище возможно с использованием стандартных протоколов передачи данных.

Что касается систем предотвращения потерь информации в корпоративной информационной системе, то они представляют собой громоздкие комплексы, которые в свою очередь делятся на подкомпоненты, закрывающие двери в информационном периметре.

От классических к многоагентным системам защиты информации. Классические информационные системы строятся по принципу создания жесткой функциональности приложения,

которая позволяет решать определенный, достаточно узкий круг задач.

Например, в системах защиты корпоративной информации может существовать модуль слежки за корпоративной почтой, который агрегирует подозрительные письма в определенное хранилище. Через определенное время хранилище просматривает специалист по информационной безопасности и делает выводы об опасности письма. В случае, если передача сведений представляет угрозу для предприятия, то к нарушителю принимаются соответствующие меры.

В данной ситуации прослеживается момент принятия решения. Этот момент разрешает специалист по информационной безопасности. Однако, механизм принятия решения возможно поручить программе, обладающей некоторыми знаниями в области принятия решений – агенту. Если спроектировать систему таким образом, она перейдет от классической формы к многоагентной.

В классической теории искусственного интеллекта решение какой-либо задачи сводится к созданию некоторой одной интеллектуальной системы, называемой агентом, которая, имея в своем распоряжении все необходимые знания, способности и вычислительные ресурсы, способна решить некоторую глобальную проблему.

В теории многоагентных систем (также часто встречается название «мультиагентные системы») за основу берется противоположный принцип. Считается, что один агент владеет всего лишь частичным представлением о глобальной проблеме, а значит, он может решить лишь некоторую часть общей задачи. В связи с этим для решения сложной задачи необходимо создать некоторое множество агентов и организовать между ними эффективное взаимодействие, что позволит построить единую многоагентную систему.

В многоагентных системах весь спектр задач по определенным правилам распределяется между всеми агентами, каждый из которых считается членом организации или группы. Распределение заданий означает присвоение каждому агенту некоторой роли, сложность которой определяется исходя из возможностей агента.

Для организации процесса распределения задачи в многоагентных системах создается либо система распределенного решения проблемы либо децентрализованный искусственный интеллект. В первом варианте процесс декомпозиции глобальной задачи и обратный процесс композиции найденных решений происходит под управлением некоторого единого «центра».

При этом многоагентная система проектируется строго сверху вниз, исходя из ролей определенных для агентов и результатов разбиения глобальной задачи на подзадачи [2].

В случае использования децентрализованного искусственного интеллекта распределение заданий происходит в процессе взаимодействия агентов и носит больше спонтанный характер. Нередко это приводит к появлению в многоагентных системах резонансных, синергетических эффектов.

Технология многоагентных систем, хотя и насчитывает уже более чем десятилетнюю историю своего активного развития, находится в настоящее время еще в стадии становления.

Ведутся активные исследования в области теоретических основ формализации основных понятий и компонент систем, в особенности в области формализации ментальных понятий [5].

Основные достижения в этой части пока не очень ориентируются на аспекты практической реализации и пока далеки от практики. В частности, при формализации ментальных понятий полностью игнорируются все разработанные в искусственном интеллекте подходы для работы с плохо структурируемыми понятиями, не вполне определенными понятиями, методы, которые базируются на вероятность и нечеткость. Представляется, что это обширное, новое и чистое поле деятельности для соответствующих специалистов [17].

Многоагентные системы. В сообществе специалистов по мультиагентным системам как одна из перспективных моделей рассматривается модель самообучающегося агента. Однако при этом делаются ссылки на результаты в области извлечения знаний и машинного обучения, полученные ранее в искусственном интеллекте применительно к экспертным системам [4].

Очевидно, что применительно к мультиагентной системе задача обучения имеет много специфики по сравнению с задачами в общей постановке, однако, эта специфика пока не изучается и не ведутся исследования по этой проблеме. Весьма специфична и задача обучения агентов коллективному поведению, ведь кооперативное решение задач подразумевает совместное использование знаний нескольких агентов. Этот вопрос тоже пока остается вне поля зрения специалистов по мультиагентным системам.

Работы в области многоагентных систем, в особенности разработка приложений, требуют привлечение знаний и технологий из ряда областей, которые ранее были вне поля зрения специалистов по искусственному интеллекту. Прежде всего это относится к параллельным вычислениям, технологии открытой распределенной обработки, обеспечения безопасности и мобильности агентов [3].

Технология мультиагентных систем не является просто объединением различных результатов в области искусственного интеллекта. Интеграция, которая приводит к парадигме многоагентных систем, привносит ряд принципиально новых свойств и возможностей в информационные технологии и по существу представляет собой качественно новый, более высокий уровень ее развития, тот

уровень, который позволяет прогнозировать ее ведущее положение в ближайшие десятилетия. Специалистам в области искусственного интеллекта здесь принадлежит ведущая роль.

Заключение. В результате проведенных исследований возможно сделать вывод, что многоагентные системы все больше проникают в область разработки программного обеспечения, однако сложность реализации интеллектуальных алгоритмов создает высокий порог по созданию таких систем.

СПИСОК ЛИТЕРАТУРЫ

1. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003, 212 с.
2. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям – М.: Эдиториал УРСС, 2002, 352с.
3. Jacques Ferber, Multi-Agent Systems: An Introduction to Artificial Intelligence, Addison-Wesley, 1999, ISBN 0-201-36048-9.
4. Michael Wooldridge, An Introduction to MultiAgent Systems, John Wiley & Sons Ltd, 2002, paperback, 366 pages, ISBN 0-471-49691-X.
5. Ron Sun and Isaac Naveh. Simulating Organizational Decision-Making Using a Cognitively Realistic Agent Model, Journal of Artificial Societies and Social Simulation.
6. http://habrahabr.ru/company/pt/blog/255681/
7. http://habrahabr.ru/post/200894/
8. http://habrahabr.ru/post/201058/
9. http://habrahabr.ru/post/258685/
10. http://geektimes.ru/post/137076/
11. http://habrahabr.ru/post/213209/
12. http://citforum.ru/security/articles/metodika_zashity/
13. http://habrahabr.ru/post/141000/
14. http://habrahabr.ru/company/pentestit/blog/263665/
15. http://www.cnews.ru/articles/kak_obespechit_informatsionnuyu_bezopasnost
16. http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf
17. http://www.aiportal.ru/articles/multiagent-systems/multiagent-systems.html

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И БИЗНЕСЕ

УДК 681.324

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИОННЫХ УСЛУГ РЕАЛЬНОГО ВРЕМЕНИ В УСЛОВИЯХ ОШИБОК, ОТКАЗОВ И ДИСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Богатырев Владимир Анатольевич[1], Богатырев Анатолий Владимирович[2],
[1.]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21.,
[2.] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверский пр., д. 49,
e-mails: Vladimir.bogatyrev@gmail.com, ganglion@gmail.com

***Аннотация*:** Для информационных систем проанализированы возможности повышение экономической эффективности предоставления информационных услуг в реальном времени в результате адаптивной реконфигурации системы, предусматривающей переключение в холодный резерв узлов, избыточных для обеспечения своевременности и безошибочности услуг с учетом угроз деструктивных воздействий, приводящих к увеличению загрузки системы.

Ключевые слова: *энергосбережение, надежность, кластер, реальное время, оптимизация, реконфигурация, информационная услуга.*

ECONOMIC EFFICIENCY OF INFORMATION SERVICES REAL-TIME ERROR CONDITIONS, FAILURES AND DESTRUCTIVE INFLUENCES

Vladimir Bogatyrev[1],Anatolij Bogatyrev[2],
[1.]Saint-petersburg state university of economics,
Russia, St. Petersburg, Sadovaya str. 21,
[2.]Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky pr., 49,
e-mails: Vladimir.bogatyrev@gmail.com, ganglion@gmail.com

Abstract: information systems are analyzed the possibilities of improving the economic efficiency of providing information services in real time in the result the adaptive reconfiguration of the system with the switch in Holodny reserve units, excess to ensure timely and error-free services with regard to threats of destructive influences, leading to increased system load.

Keywords: *energy saving, reliability, cluster, real time, optimization, reconfiguration, information service.*

Введение. Эффективность информационного сервиса, в том числе его экономическая эффективность, во многом определяется уровнем информационной безопасности, надежности, отказоустойчивости, энергопотребления и производительности компьютерных систем [1],.[2],[3],[4], [5].

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, снижение потенциально достижимого в результате резервирования уровня надежности (в том числе в результате повышения тепловыделения, приводящего к росту интенсивности отказов) и, в итоге, к снижению экономической эффективности предоставления информационных услуг.

Для уменьшения отрицательного влияния резервирования компьютеров на рост энергопотребления могут применяться [6]: кондиционирование и охлаждение; микропроцессоры и другие электронные компоненты с низким напряжением питания и энергопотреблением; хранение данных на базе флэш-памяти с низким энергопотреблением; Blade серверы и другие решения.

Эффективность использования резервированных информационно вычислительных ресурсов, достигается при их консолидации в кластеры. Консолидация ресурсов хранения и обработки данных в кластерах позволяет реализовать динамическое распределение запросов на предоставление

информационных услуг при адаптации системы к накоплению отказов и изменениям входной нагрузки [7], [8].

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 [9], [10].

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 (происходящего случайно или преднамеренно вследствие DDOS-атак, то есть атак направленных на увеличение загрузки компьютерных узлов и нарушению стационарности процессов обслуживания) происходит адаптивное подключение в работу необходимого числа узлов, находящихся в холодном резерве. В случае же снижения нагрузки часть активных узлов переключается в холодный резерв [11]. Для кластерных систем большей гибкости и соответственно больших возможностей адаптивной реконфигурации потенциально можно достичь при объединении в кластер большего числа более простых и дешевых компьютерных узлов, в том числе на основе технологии Blade-серверов, которые имеют встроенные системы управления охлаждением и электропитанием [6].

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 DDOS-атакам.

Для повышения устойчивости к отказам и ошибкам вычислительного процесса в кластерных компьютерных 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 [12], [13].

Таким образом, представляется актуальным исследование возможностей адаптивной энергосберегающей реконфигурации кластерных систем, которая потенциально может привести к повышению экономической эффективность предоставления информационных услуг реального времени, когда стоимость услуги зависит от задержки ее предоставления [13].

Рассмотрим вычислительную систему кластерной архитектуры, предназначенную для предоставления информационных услуг в реальном времени в условиях сбоев, отказов и ошибок.

Кластерная система объединяет n однотипных взаимозаменяемых серверов, представимых одноканальными системами массового обслуживания с бесконечной очередью. 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. Среднее время обслуживания запросов во всех узлах будем считать одинаковым и равным v.

Будем полагать, что при предоставлении информационных услуг в реальном времени, прибыль от безошибочного выполнения каждого запроса, если время его ожидания была меньше t_0 равна a_1, а если больше t_0 или результат ошибочный, то налагается штраф равный a_2, при этом расходы на электропитание каждого узла в единицу времени равны a_3.

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.

Достижение поставленной цели сопряжено с:

– построением 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;

– постановкой и решением задачи поиска оптимального числа отключаемых узлов (переключаемых в холодный резерв), позволяющего максимизировать эффект от предоставления услуг в реальном времени с учетом затрат на энергопотребление.

Эффективности предоставления информационных услуг. Прибыль от предоставления информационных услуг, получаемую в единицу времени, при адаптивной энергосберегающей реконфигурации определим как [11]:

$$A = \Lambda b(Pa_1 - (1-P)a_2) - a_3(n-k),$$

$$A_1 = \Lambda b(P_1 a_1 - (1-P)a_2) - a_3(n),$$

где:

b – доля потока запросов, принимаемых кластером к обслуживанию;

k – число отключенных узлов (находящихся в холодном резерве);

P, P_1 – вероятности своевременного получения безошибочных результатов для систем с реконфигурацией (адаптивного переключения узлов в холодный резерв) и без нее.

При этом $P = rp, P_1 = r_1 p$, где p – вероятность того, что за время $t = t_0 + v$ от поступления запроса до выдачи результата, отказы, сбои и ошибки не возникают;

r, r_1 – вероятности того, что время ожидания запросов в очереди узла меньшее предельно допустимого значения t_0 для кластеров с реконфигурацией и без нее.

$$r = 1 - (vb\Lambda/(n-k))\exp(-t(v^{-1} - b\Lambda/(n-k), \quad r_1 = 1 - (vb\Lambda/n)\exp(-t_0(v^{-1} - b\Lambda/n),$$

$$p = \exp(-\lambda(t_0 + v),$$

где

$b\Lambda$ – интенсивность потока запросов, принимаемая в кластер на обслуживание, а

λ – суммарная интенсивность отказов и ошибок вычислений в одном узле.

При значительности штрафов от неполучения или задержки результатов принятых к обслуживанию запросов для увеличения вероятности своевременного и безошибочного обслуживания в реальном времени в [12], [13] предлагается резервированное выполнение запросов в разных узлах кластера. В этом случае, если достаточно получение безошибочного результата хотя бы в одном из d узлов, принимающих запрос к резервированному обслуживанию, то

$$P = 1 - (1 - rp)^d, \quad P_1 = 1 - (1 - r_1 p)^d,$$

где

r, r_1 – вероятности того, что время ожидания запросов в очереди узла меньшее предельно допустимого значения

t_0 – соответственно для кластеров с реконфигурацией и без нее рассчитываются с учетом возрастания загрузки узлов в результате резервирования запросов (выполнения d копий запросов).

$$r = 1 - (vb\Lambda d/(n-k))\exp(-t_0(v^{-1} - db\Lambda/n-k),$$

$$r_1 = 1 - (vb\Lambda d/n)\exp(-t_0(v^{-1} - bd\Lambda/n).$$

В результате оптимизации при заданной интенсивности потока запросов Λ требуется определить число отключаемых компьютерных узлов в кластере (переключаемых в холодный резерв) k, и долю принимаемых к обслуживанию запросов.

Критерий оптимизации – максимум A прибыли от предоставления информационных услуг Max(A) с учетом затрат на энергопотребление при условии обеспечения стационарности процесса обслуживания $vb\Lambda/(n-k) < 1$ без резервирования обслуживания запросов и $vb\Lambda d/(n-k) < 1$ при их резервировании.

При оптимизации кластера без энергосберегающей реконфигурации определяется только доля принимаемых к обслуживанию запросов, для которой достигается максимум доходов от предоставления услуг Max(A) при условии стационарности $vb\Lambda/n < 1$.

Приведем пример оптимизации процесса предоставления информационных услуг реального времени без резервирования запросов в зависимости от интенсивности входного потока Λ, для кластера, содержащего n =15 серверов. Расчеты проведем для предельно допустимого времени

ожидания запросов в очереди t_0 =2 с, среднем времени обслуживания запросов ν =1 с, a_1 =1 у.е., a_2 = 2 у.е. и a_3 =0,1у.е.

Результаты расчетов представлены на рисунке 1, на котором кривая 1 соответствует оптимальным значениям доли подключенных узлов $K = k/n$ при реконфигурации кластера, кривая 2 соответствует оптимальной доли b запросов, принимаемых к обслуживанию кластером.

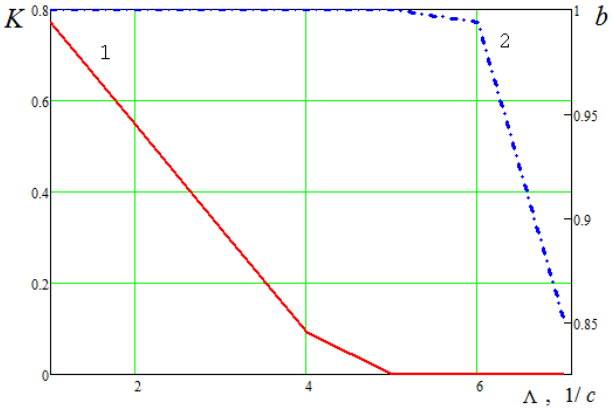


Рис. 1. Оптимальная доля, подключенных узлов при реконфигурации кластера

Результаты оценки эффективности предоставления информационных услуг представлены на рисунке 2, на котором кривая 1 соответствует кластеру с адаптивной реконфигурацией при оптимальных значениях параметров b и k, а кривая 2 – кластеру без реконфигурации при оптимизации доли принимаемых к обслуживанию запросов b. Результаты расчетов показывают высокую эффективность энергосберегающей реконфигурации особенно при низкой загрузке системы.

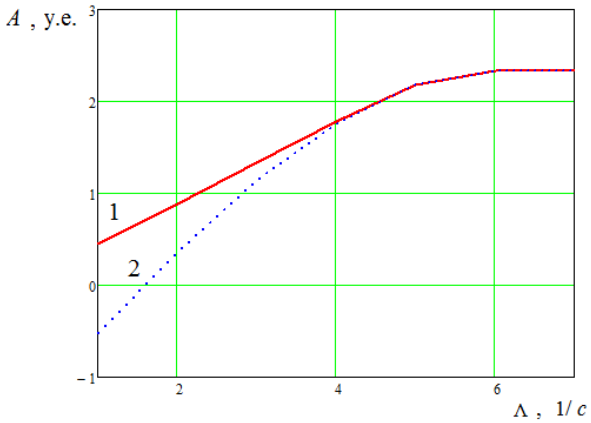


Рис. 2. Эффективность реконфигурируемого кластера при оптимальных параметрах k и b

Таким образом, для кластерных систем реального времени, консолидирующих ресурсы серверов, оценена эффективность адаптивной энергосберегающей реконфигурации, основанной на отключении (переключении в холодный резерв) компьютерных узлов избыточных для обеспечения требуемого качества услуг.

Заключение. Показана высокая эффективность энергосберегающей реконфигурации особенно при низкой загрузке системы. Предложена модель кластера, позволяющая оценить эффективность предоставления информационных услуг реального времени в зависимости от интенсивности входного потока и числа активных узлов кластера и кратности резервного обслуживания запросов. Решена задача оптимальной реконфигурации кластера с адаптивным переключением части узлов в холодный резерв, с целью максимизации эффекта от предоставления услуг в реальном времени с учетом их своевременности и издержек на энергопотребление.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 92–95.
2. Воробьёв А.И., Колбанёв М.О., Татарникова Т.М. Оценка вероятностно-временных характеристик процесса предоставления информационно-справочных услуг //. Известия высших учебных заведений. Приборостроение. 2014. т. 57. № 9. С. 15-18.
3. Коршунов И.Л. Состояние и концепция развития информационных технологий в сфере сервиса//Известия высших учебных заведений. Приборостроение. 2014. т. 57. № 9. с. 7-10
4. Микадзе С.Ю., Колбанёв М.О., Татарникова Т.М. Модель информационного взаимодействия для предприятий сервиса //Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 10-14.

5. Bogatyrev V.A., Bogatyrev S.V., Golubev I.Yu. Optimization and the process of task distribution between computer system clusters // Automatic Control and Computer Sciences. 2012. V. 84. № 3. P. 103–111. doi: 10.3103/S0146411612030029
6. Энергосбережение в сфере компьютерных технологий: мифы и реальность. http://www.dltens.ru/energosberegteh.html
7. Богатырев В.А. Надежность вариантов размещения функциональных ресурсов в однородных вычислительных сетях//Электронное моделирование. 1997. № 3. С. 21-29.
8. Богатырев В.А. К распределению функциональных ресурсов в отказоустойчивых многомашинных вычислительных системах//Приборы и системы. Управление, контроль, диагностика. -2001. -№ 12. С. 1–5.
9. Богатырев В.А., Богатырев С.В. Объединение резервированных серверов в кластеры высоконадежной компьютерной системы//Информационные технологии. 2009. № 6. С. 41-47.
10. Богатырев В. А. Мультипроцессорные системы с динамическим перераспределением запросов через общую магистраль // Изв. Вузов. Приборостроение. 1985. № 3. С.33–38.
11. Богатырев В.А., Богатырев А.В Кластеры предоставления информационных услуг с энергосберегающей реконфигурацией. // Технико-технологические проблемы сервиса. 2014. № 4 (30). С. 38–41.
12. Bogatyrev V.A., Bogatyrev A.V. Functional Reliability of a Real-Time Redundant Computational Process in Cluster Architecture Systems. Automatic Control and Computer Sciences. 2015. Vol. 49. № 1. pp. 46-56. DOI 10.3103/S0146411615010022
13. Богатырев В.А., Богатырев А.В. Оптимизация резервированного распределения запросов в кластерных системах реального времен // Информационные технологии № 7. Том 21. 2015. С. 495–502.

УДК 339.9.01

ТРАНСПОРТНЫЙ ФАКТОР КАК ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Васькова Анастасия Викторовна, Михайличенко Екатерина Михайловна,
ФГОБУ ВПО «Финансовый университет при Правительстве Российской Федерации»,
Россия, Санкт-Петербург, ул. Съжжинская д. 15-17,
e-mails: k89897218915@yandex.ru, nastya-363@ yandex.ru

Аннотация: В статье рассмотрены проблемы железнодорожного транспорта. В аспекте обеспечения национальной экономической безопасности, как важной оценки роли железнодорожного транспорта в устойчивом функционировании стратегических отраслей материального производства, которое нуждается в перевозках собственной продукции. Был сделан вывод, что в отрасли существуют угрозы экономической безопасности. Несмотря на активную политику руководства отрасли и принятие ряда эффективных мер по устранению негативных тенденций, принесших положительный результат, ситуацию с обеспечением устойчивой работы железнодорожного транспорта в долгосрочной перспективе нельзя признать удовлетворительной. В связи с этим становится очевидной необходимость эффективного механизма обеспечения экономической безопасности отрасли, включая разработку пороговых значений индикаторов, организацию постоянного мониторинга экономической ситуации и принятие управляющих воздействий, нейтрализующих выявленные угрозы экономической безопасности.

Ключевые слова: *транспортный комплекс; экономическая безопасность; социальная сфера; железнодорожный транспорт; рыночные отношения.*

TRANSPORT FACTOR AS A MEASURE OF ECONOMIC SECURITY

Vaskova Anastasia Viktorovna, Mikhailichenko Ekaterina Mikhailovna,
FGOBU VPO «Financial University under the Government of the Russian Federation»,
Russia, St. Petersburg, Street Sytinsky 15-17,
e-mails: k89897218915@yandex.ru, nastya-363@ yandex.ru

Abstract: The problems of railway transport. In the aspect of national economic security is important to evaluate the role of rail transport in the sustainable functioning of the strategic sectors of material production, which needs to transport its own products. It was concluded that the industry is under threat of economic security. In spite of an active policy management industry and the adoption of a series of effective measures to eliminate the negative tendentsy, brought a positive result, the situation with the provision ustoychivoy of rail transport in the long term can not be considered satisfactory. In this regard, it becomes apparent neobhodimost effective mechanism to ensure the economic security of arias, including the development of threshold values of indicators, the organization monitoring the economic situation and the adoption of Governors vozdeystvy neutralizing the identified threat of economic security.

Keywords: *transport complex; economic security; social services; railway transport; market relations.*

Введение. 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 регионов в страны. Транспортная сеть является звеном, которое связывает производителей и потребителей продукции, товаров, услуг, без которых невозможно существование 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 себя большой 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 продукте страны на 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 имеет ведущее значение для хозяйственных связей и платежеспособности граждан [2]. Железные дороги в процентном соотношении для системы транспорта общего пользования составляет 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 обеспечения крупномасштабных пассажирских перевозок при четко установленном уровне тарифов, с убыточностью до 50–60% (таблица 1).

Таблица 1

Технические характеристики ОАО «РЖД»

Эксплуатационная длина железных дорог	85,2 тыс. км
Протяженность электрифицированных линий	43,3 тыс. км
Доля в грузообороте транспортной системы России	43,2%*
Доля в пассажирообороте транспортной системы России	28,6%

Примечание: *С учетом трубопроводного транспорта.

Из вышеперечисленного можно сделать вывод, что железнодорожный транспорт обеспечивает устойчивое развитие материального производства, быстрое увеличение эффективного расходования ресурсов, эффективное сокращение себестоимости продукции при уменьшении транспортного бремя, обильный рост активности, а так же способствует быстрому решению других социальных задач. При этом из-за нехватки развития транспортных связей существуют большие потери в народном секторе. Железнодорожный вид транспорта в условиях развития современной России нельзя считать конкурирующим с автомобильным видом транспорта во внутригосударственных перевозках [8].

В результате проведенного сравнительного анализа по различным видам транспорта можно сказать следующее, что по абсолютному числу погибших, железнодорожный сектор считается одним из самых безопасных видов внутригосударственного транспорта.

Таблица 2

Число погибших на 10 тыс. транспортных средств

	Число погибших на 10 тыс. транспортных средств,(человек)		
	2012	2013	2014
	январь-декабрь	январь-декабрь	январь-декабрь
Российская Федерация	120,98	5,07	4,84

Примечание: *к набору данных применены пользовательские настройки.

По данным таблицы 2 можно сказать следующее, что самое большое количество смертей приходилось 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.

В результате постоянного изменения уровня рентабельности работы транспортного сектора, которая характеризуется зависимостью от состояния безопасности движения поездов, данная экономическая оценка трактуется как негативная тенденция. По предварительным расчетам коэффициент потерь, от перечня отраслей, которые не входят в основной спектр, требует предварительной корректировки уровня рентабельности отрасли, в размере 0,5–1,0% в сторону снижения [4]. При принятии во внимание огромные потери дорог и время по ремонту, то снижение в процентном показателе будет равно 1,5–2%, или в суммарном денежном показателе более чем 5–6 млрд. руб. В результате этого, средства, которые были выделены на повышение безопасности движения поездов – это необходимый вклад в достижение устойчивости и увеличения эффективности работы транспорта железнодорожного сектора. Результаты такого исследования

дают точную оценку влияния уровня безопасности движения транспорта на экономическое положение той или иной отрасли [7].

Самая критическая ситуация приходится на износ активной части основных фондов железнодорожного транспорта, к ним относится: электровозы данный показатель составил 72%, тепловозы – 81,5%; показатель износа по грузовым вагонам за последние 10 лет возрос почти в два раза (с 32% до 71,5%), а пассажирских вагонов – более чем в три раза.

Угрозы в социальной сфере – это обязательный аспект устойчивого положения и работы железнодорожного транспорта, как сложного технологического комплекса и кадрового потенциала отрасли [6].

В результате этого можно выделить следующий ряд угроз экономической безопасности, который, прежде всего, связан с уровнем оплаты труда.

Таблица 3

Уровень среднемесячной заработной платы относительно железнодорожного транспорта, %

Отрасль	2001	2013	Место в экономике
Газовая	232	355	1
Нефтедобывающая	170	308	2
Финансы, кредит, страхование	92	201	3
Цветная металлургия	127	177	4
Нефтеперерабатывающая	129	173	5
Геология	82	149	6
Электроэнергетика	118	127	7
Угольная	135	119	8
Черная металлургия	77	103	9
Информационно-вычислительное обслуживание	49	103	10
Железнодорожный транспорт	100	100	11

Данные таблицы 3 говорят нам о том, что среднемесячная заработная плата работника железнодорожного транспорта по отношению к другим отраслям, занимает 11 место в экономике. Всего на 3% заработная плата работников черной металлургии и информационно-вычислительного обслуживания отличается от работников транспортной сферы [1].

Удельный вес каждой из категорий персонала в общей численности определяется в следующем процентном отношении:

– рабочие – 68,6% (670 088 человек);
– специалисты – 20,8% (202 964 человека);
– руководители – 6,9% (67 417 человек);
– служащие – 3,7% (35 647 человек).

Уровень образования персонала в ОАО «РЖД»:

– работники с высшим образованием – 22,2% от общей численности, данный показатель увеличился к началу года на 1,3%;

– со средним профессиональным образованием численность работников составляет 25,7%, к началу года показатель увеличился на 0,2%.

Основную долю работников организации составляют молодые работники в возрасте до 30 лет, данный показатель увеличилась за год на 1,1% и на данный момент составляет 28%. Средний возраст работников компании «РЖД» составляет 39,5 лет.

Из общей численности работников женщины составляют 286 339 человек. В процентном показателе это 30,4%. Так же женщины занимают 51,7% руководящих должностей и специалистов, и их численность с каждым годом растет и на данный момент составляет 138,3 тыс. человек.

Угрозы в финансовой сфере – это ключевой фактор, который влияет на финансовое положение отрасли, и говорит об убыточности пассажирских перевозок.

В пригородном сообщении пассажиры оплачивают не более 20% от стоимости проезда, 7–10% покрывают региональные бюджеты, остальная часть, это так называемые, эксплуатационные расходы, т.е. те расходы, которые оплачиваются за счет доходов от грузовых перевозок. Так как все правовые документы носят рекомендательный, а не директивный характер, то действующая нормативно-правовая база в Российской Федерации, предусматривает компенсацию потерь бюджетными средствами, но не решает проблему убыточности пригородных перевозок. В результате этого даже при заключении большого количества контрактов с регионами будут исполняться не в полном объеме [9].

Негативное влияние на российскую экономику в 2014 году оказали такие показатели как: резкое снижение цен на необработанную нефть; значительная девальвация российского рубля; санкции, введенные против России. Уже в декабре 2014 года процентные ставки увеличились, по средствам,

поднятия Центральным Банком ключевой ставки до 17%. Совокупность данных показателей способствовала: снижению доступности капитала; повышению стоимости капитала; росту инфляции.

В начале декабре 2014 года, в соответствии с прогнозом социально-экономического развития России на 2015-2017 года, который утвержден Правительством РФ, был опубликован следующий рост тарифов на грузовые железнодорожные перевозки:

– в 2015 году на 10%;
– в 2016 году на 5,5%;
– в 2017 году на 4,5%.

По средствам этого, в транспортной сфере существуют множество угроз, которые влияют на экономическую безопасность в каждой сфер деятельности. Несмотря на проведение активной политики руководства отраслей и принятие ряда положительных мер по устранению негативной стороны, которые принесли исключительно положительный результат, данную ситуацию по обеспечению устойчивой работы железнодорожной сферы на долгосрочную перспективу, ни в коем случае, нельзя признать удовлетворительной. В результате этого становится очевидным необходимость разработка эффективного механизма обеспечения экономической безопасности разных отраслей [3].

Заключение: Положительные сдвиги в экономике страны определяются необходимостью эффективного развития транспортного комплекса, что говорит о ее устойчивой работе, потенциале растущего платежеспособного спроса граждан, доступности и высоком качестве предоставляемых услуг, снижение себестоимости на перевозки пассажиров и грузов. Решение поставленных задач в итоге, будет обеспечивать транспортную составляющую национальной экономической безопасности [4].

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, вследствие неэффективного применения элементов нового оборудования, а так же современного научно-технического прогресса.

б) в социальной сфере определяется:

– постоянно прогрессирующим несоответствием в заработной плате в транспортной сфере и в базовых отраслях, что приводит к высокому уровню текучести кадров;

– недостаточным стимулированием работников для получения максимального результата, в частности это соотношение между ростом производительности труда и ростом заработной платы;

– неоправданной разницей 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.

СПИСОК ЛИТЕРАТУРЫ

1. Бевзюк Е.А. Комментарий к Федеральному закону от 09.02.2007 № 16-ФЗ «О транспортной безопасности» (постатейный). 2013, 452 с.
2. Комарова Т.М. Уровень преступности как фактор социально-демографической безопасности региона. 2014, 132-134с.
3. Концепция транспортной безопасности Российской Федерации // Министерство транспорта Российской Федерации. 2014г.
4. Пекарская О.А.. В сборнике: Журнал правовых и экономических исследований, 2012,162-165с.
5. Пекарская О.А.. Журнал правовых и экономических исследований, 2015, 184-188с.
6. Талыбов Д.Р. Транспортная система России: современное состояние и проблемы развития. 2014, 81-85с.
7. Транспорт в России, // Федеральная служба государственной статистики. 2013, 368с.
8. Экономическая безопасность / Под ред. В.А. Богомолова. – М.: ЮНИТИ-ДАНА, 2015, 295с.
9. Экономическая безопасность России / Под ред. В.К. Сенчагова. – М.: Дело, 2013, 896с.

УДК 004.75

НЕКОТОРЫЕ АСПЕКТЫ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д 21,
e-mails: dina_25@hotbox.ru, mokolbanev@mail.ru.

Аннотация: Рассматривается влияние длины передаваемого блока информации на вероятностно-временные характеристики и энергопотребление сети пакетной передачи.

Ключевые слова: *энергоэффективность; длина передаваемого блока информации; вероятностно-временные характеристики.*

SOME ASPECTS OF ENERGY EFFECTIVE COMMUNICATION

Verzun Natalia, Kolbanev Mikhail,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mails: dina_25@hotbox.ru,mokolbanev@mail.ru.

Abstract: Considered the effect of the length of the transmitted information block on the probability-temporal characteristics and energy consumption packet network.

Keywords: *energy efficiency; length of the transmitted information block; probability-temporal characteristics.*

Введение. Современные информационные системы, применяемые во всех сферах экономической деятельности, характеризуются территориально распределенной структурой, необходимостью передачи и хранения значительных объемов информации, большим количеством пользователей и сложными схемами их взаимодействия. При создании подобных систем необходимо уделять внимание обеспечению информационной безопасности[1],[2],[3],[4], надежности[5],[6], атакже эффективности использования физических и информационных ресурсов[7],[8]. Последний аспект становится все более актуальным в связи с ростом объемов передаваемой ихранимой информации. Обеспечение доступности информационных и экономии физических ресурсов становится одной из основных задач специалистов в области информационных технологий.

Физические ресурсы информационного взаимодействия включают в себя пространственные, временные и энергетические ресурсы. Энергия при информационном взаимодействии затрачивается на всех его этапах. В данной работе остановимся подробнее на этапе передачи информации.Одним из путей повышения энергоэффективности процесса обмена информацией является рациональный выбор алгоритмов управления информационными потоками, в частности, алгоритмов передачи, доступа к среде передачи, режимов передачи и обработки служебной информации, выбор эффективной длины передаваемых блоков и др. Рассмотрим влияниедлины передаваемого блока(ДПБ) информации в локальной сети передачи данных(ЛСПД) на вероятностно-временные(ВВХ) и энергетические характеристики(ЭХ) передачи файла по ЛСПД.

1.Вероятностно-временные и энергетические характеристики передачи информации. Предположим: ЛСПД однородна и включает в себя N станций пользователей. На вход каждой станции поступают бернуллиевские потоки пакетов с параметром $q_и$ на интервале T_0 ($T_0 = 1/V_с$, $V_с$ – скорость передачи (бит/с)), метод доступа – синхронный временной доступ(СВД), топология – шина, используется режим пакетной передачи и файл длиной F (бит) разбивается при передаче(на транспортном уровне OSI)на равные блокидлиной s (бит).

Ранее рассматривались математические модели различных ЛСПД, а также предлагались методы расчета их ВВХ [9,10].Для выбора ДПБ рассмотрим следующиеВВХ для ЛСПД с СВД:

$\overline{\Pi_q}$ – вероятность своевременной доставки пакета по ЛСПД:

$$\overline{\Pi_q} = f_q(z)\Big|_{z=Q_д^{-1}},\ Q_д = 1 - T/\overline{T_д}, \qquad (1)$$

где $f_q(z)$ – z-преобразование ряда распределения времени задержки информации. $\overline{T_д}$ – среднее допустимое время доставки пакета.

$\overline{\Pi_{qф}}$ – вероятность своевременной доставки файла длиной F, разбитого на блоки длиной s

$$\overline{\Pi_{qф}}(F,s) = \overline{\Pi_q}^{[F/s]} \qquad (2)$$

Энергозатраты на передачу информации пользователя складываются в общем случае иззатрат: на формирование линейного кода для транспортировки данных по сети, непосредственно на передачу,на обработку адресной и другой служебной информации(СИ).Введем характеристику(ЭХ), которая позволитоценить эффективность ЛСПД с точки зрения затрат энергии на обработку СИ -доля СИ, приходящаяся на 1 бит передаваемого файла длиной F, в случае его разбивки наблоки длиной s

$$\delta = (B_{\text{СИ}}/F)\cdot 100\%,\ \ B_{\text{СИ}} = \left[F/s\right]\cdot r_{\text{СИ}}(\text{бит}),$$
$$r_{\text{СИ}} = r_{\text{су}} + r_{\text{ту}} + r_{\text{ф}} + r_{\text{а}} + r_{\text{у}} + r_{\text{кр}} + r_{\text{пр}} + n_{\text{кв}}(\text{бит}), \qquad (3)$$

где $B_{\text{СИ}}$ - количество СИ приходящейся на передачу файла длины F в случае его разбивки на блоки длиной s, $r_{\text{СИ}}$ – количество бит в передаваемых служебных полях и квитанций, $r_{\text{пр}}$ – длина преамбулы (бит), $r_{\text{ф}}$ – длина флага(бит), $r_{\text{а}}$ – длина поля адреса(бит), $r_{\text{у}}$ – длина поля управления (бит), $r_{\text{кр}}$ – длина поля контрольных разрядов(бит), $r_{\text{ту}}$ – длина заголовка транспортного уровня(бит) и $r_{\text{су}}$ – длина заголовка сетевого уровня (бит), $n_{\text{кв}}$ – длина квитанции(бит).

2.Расчет характеристик ЛСПД. Проведем расчетВВХ и ЭХ передачи файла по ЛСПД и выявим их зависимость от ДПБ (s – информационной части протокольного блока транспортного уровня). Для расчета воспользуемся методами, приведенными в [10]и выражениями (1)-(3). Исходные данные: N =20, $V_{\text{с}}$ =1010(бит/с), длина канала $D_{\text{к}}$ =0,2(км), время декодирования кадров и квитанции tдкк=tдккв=10-6(с), $\overline{T}_{\text{д}}$ =0,2(с), интенсивность входного потока пакетов на станцию ЛСПД $\lambda_{\text{и}}$ =15(пак/с), $n_{\text{кв}}$ =32(бит), вероятность ошибки в канале передачи p =10-4; 10-5; 10-6; 10-8, F =65536(байт), параметры передаваемых кадров: $r_{\text{ф}}$ =8(бит), $r_{\text{пр}}$ =32(бит), $r_{\text{у}}$ =16(бит), $r_{\text{кр}}$ =32(бит), $r_{\text{су}}$ =160(бит), $r_{\text{ту}}$ =160(бит), s =128; 256; 512; 1024; 2048; 4096; 8192; 16384; 32876; 65536 байт.

Графики характеристикприведены на рисунке1 – зависимость вероятности своевременной доставки кадра от ДПБ – $\overline{\Pi_q(s)}$, на рисунке 2 – зависимость вероятности своевременной доставки файла от ДПБ– $\overline{\Pi_{q\text{ф}}(s)}$ и от доли СИ, приходящейся на 1 бит передаваемого файла $\overline{\Pi_{q\text{ф}}(\delta)}$ при различных значениях p.

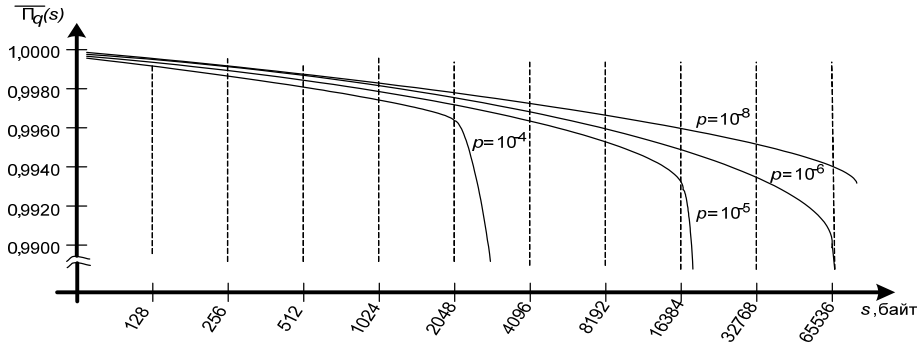


Рис. 1. Зависимость вероятности своевременной доставки кадра от ДПБ

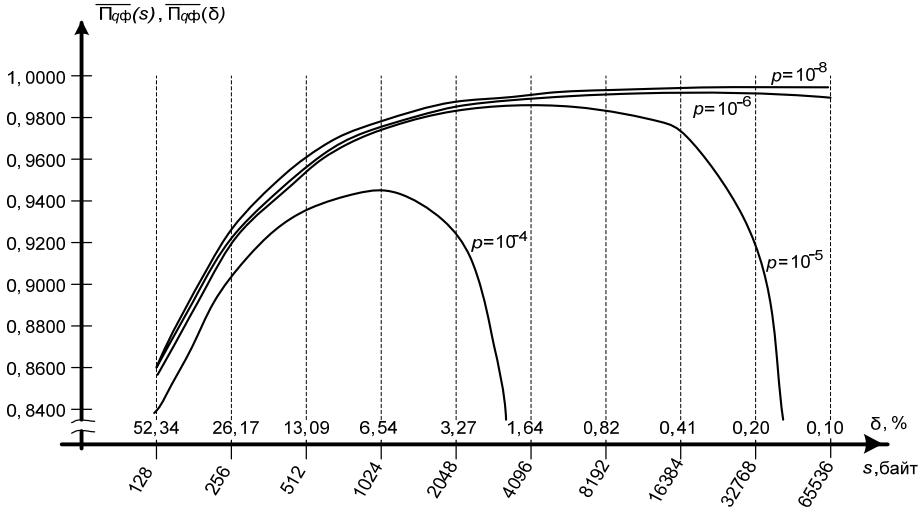


Рис. 2. Зависимость вероятности своевременной доставки файла от ДПБ и от доли служебной информации, приходящейся на 1 бит передаваемого файла

3. Анализ вероятностно-временных и энергетических характеристик. Анализируя получившиеся кривые можно сказать, что с увеличением ДПБ по ЛСПД вероятность своевременной доставки пакета уменьшается при всех рассмотренных значениях вероятности ошибки в канале передачи(см.рис.1), но вероятность своевременной доставки всего файла ведет себя не так однозначно и существенно зависит от качества канала (см. рис.2). Так,в случае низкого качества среды передачи, при вероятности ошибки p =10-4 максимум вероятности своевременной доставки файла наблюдается при s =1024 байт, если же качество среды передачи улучшается, то s благоразумнее выбирать большей длины – это позволит не только добиться увеличения вероятности своевременной доставки всего файла, но и приведет к уменьшению доли передаваемой СИ (так, например, при передаче по ЛСПД блоков длины 32768 байт, 65536 байт доля СИ составляет всего 0,2 и 0,1%), а соответственно и минимизации энергопотребления на обработку и передачу СИ.

Заключение. В современных условиях, когда назрела задача повышения ресурсной экономичности информационных технологий, необходимо проводить выбор режимов передачи, доступа к физической среде, алгоритмов передачи и обработки СИ, а также длины передаваемых блоков не только с точки зрения обеспечения необходимого качества передачи информации, как это осуществлялось ранее, но и учитывая необходимость минимизации энергетических затрат.В работе предлагается метод оценки однойсоставляющей потребленияэнергии в процессе передачи информации – затраты энергии на обработку СИ, и рассматривается влияние на них ДПБ и качества среды передачи.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т. М. Защищенные корпоративные сети: задачи по защите информации. СПб: РГГМУ, 2012. 113 с.
2. Левкин И. М. Информационные проблемы современного общества// Российская национальная библиотека, 2013, С.108–125.
3. Левкин И. М., Микадзе С. Ю. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе.Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013, С.176-177.
4. Верзун Н. А. Модель процесса передачи информации в сети с разграничением прав доступа с использованием устройства контроля доступа.Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013, С.134-135.
5. Богатырев В. А., Богатырев С. В., Богатырев А. В. Функциональная надежность вычислительных систем с перераспределением запросов // Изв. вузов. Приборостроение. 2012. Т. 55. № 10. С. 53–57.
6. Богатырев В. А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем // Информационные технологии.-1999. № 9. С. 44-48.
7. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. О развитии технологии информационного общества. Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013, С.23.
8. Колбанёв М. О., Татарникова Т. М., Воробьев А. И. Двухуровневая модель информационного взаимодействия. Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013, С.184-185.
9. Чугреев О. С., Верзун Н. А., Клевакичев С. И. Множественный доступ к доставке и обработке неоднородной информации. VI Международный форум по информатизации ISINAS-2000. – СПб., 2000. С.345-357.
10. Верзун Н. А. Множественный доступ в информационных системах. Учебное пособие. СПб.: СПбГУТ, 2007. 92 с.

УДК 004.032

ФИЗИЧЕСКИЙ ОБЪЕМ БАЗОВЫХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Колбанев Михаил Олегович, Микадзе Сегей Юрьевич, Татарникова Татьяна Михайловна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mails:mokolbanev@mail.ru,tm-tatarn@yandex.ru.

Аннотация: Приводятся основные физические ресурсы, потребляемые базовыми информационными процессами. Предлагается модель физических ресурсов в виде куба, который характеризует объем технологии, применяемой для реализации соответствующего информационного процесса. Классификация существующих информационных процессов по физическим объемам позволяет упростить задачу выбора технологии, как специалистам, так и пользователям.

Ключевые слова: *информационный процесс; физическая среда взаимодействия; физический ресур; модель физических ресурсов; технология хранения; технология распространения; технология обработки данных.*

PHYSICAL VOLUME OF BASIC INFORMATION PROCESSES

Kolbanev Mikhail, Mikadze Sergey, Tatarnikova Tatiana,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mails: mokolbanev@mail.ru, tm-tatarn@yandex.ru.

Abstract: Provides the basic physical resources consumed basic information processes. A model of physical resources in the form of a cube, which characterizes the volume of technologies used to implement the relevant information process. Classification of existing information processes in physical volumes allows to simplify the choice of technology, both for specialists and users.

Keywords: *information process; the physical environment interactions; physical resource; a model of physical resources; storage technology; data transmission technology; data processing technology.*

Введение. Любую деятельность человека сопровождает информационное взаимодействие. Оно осуществляется на двух метауровнях: идеальном, который является продуктом мышления людей и обеспечивает на передающей стороне порождение, а на приемной стороне постижение таких идеальных категорий, как смыслы, значения, образы, эмоции и материальном, который поддерживает идеальный метауровень и обеспечивает обмен данными, имеющими физическую форму представления.

На метауровнях реализуются информационные процессы. Информационные процессы идеальногометауровня обеспечивают смысловое взаимодействие людей. Информационные процессы материальногометауровня представляют собой последовательность операций над данными.

Если данные представить в виде числовых массивов, то их преобразование можно автоматизировать при помощи вычислительных (компьютерных) систем:

– выполнение комплекса операций на материальномметауровне предполагает не только перемещение определенных объемов данных между взаимодействующими сторонами, но и выполнение требований к качеству доставки. Эти требования формулируются на идеальном метауровне и могут измеряться, например, в единицах дальности, времени или достоверности доставки [3],[5],[7];

– информационное взаимодействие на обоих метауровнях поддерживается физической средой;

– среда взаимодействия призвана распространять сигнал (свойство канала связи), сохранять сигнал (свойство памяти), и изменять форму представления сигнала (свойство обработчика данных). При помощи управления можно регулировать количественные и качественные проявления этих свойств в зависимости от способа реализации информационного взаимодействия [4],[11],[17].

1. Физические ресурсы базовых информационных технологий. Поскольку данные материальны, то их преобразование подчиняется законам физики, в соответствие с которыми движение в пространстве и времени требует энергии.

Соответственно, количественную меру возможности преобразования данных физической средой взаимодействия можно задать при помощи трех типов физических ресурсов: пространственных, временных и энергетических.

В таблице1 приведены основные физические ресурсы, потребляемые базовыми информационными процессами.

Таблица 1

Физические ресурсы для базовых информационных процессов

Базовые информационные процессы	Технологические ресурсы		
	Пространственные	Временные	Энергетические
Сохранение	Плотность записи данных	Время гарантированного сохранения	Энергозатраты для сохранения бита
Распространение	Зона охвата	Время доставки данных	Энергозатраты для перемещения бита
Обработка	Размер техпроцесса	Производительность	Энергозатраты для изменения бита

Плотность записи данных – это количество бит, которое размещается на единице площади (или объема) запоминающего устройства.

Зона охвата – это территория, в пределах которой организуется информационное взаимодействие пользователей и распределение пользователей по этой территории.

Техпроцесс – это последовательность технологических операций изготовления транзисторов и других полупроводников.

Время гарантированного сохранения – это период времени, который начинается в момент записи данных на ЗУ и продолжается до тех пор, пока данные могут быть: 1) найдены на ЗУ, 2) считаны и 3) интерпретированы пользователем.

Время доставки данных – это время, это период времени, который начинается в момент поступления сигнала в канал связи и заканчивается по достижению данными заданной точки пространства (адресата).

Производительность – это количество операций обработки за единицу времени.

Энергозатраты для сохранения – это энергетический барьер, которым должны быть отделены друг от друга минимальные единицы хранения данных.

Энергозатраты для распространения – это уровень отношения «сигнал/шум», который нужно поддерживать для перемещения одного бита.

Энергозатраты для обработки – это энергия, которая расходуется на обработку одного бита при соответствующем технологическом процессе.

Эти ресурсы связаны друг с другом. Например, при магнитной записи увеличение плотности записи ведет к сокращению времени гарантированного сохранения. Увеличение зоны охвата увеличивает время перемещения данных и энергозатраты на восстановление затухающего сигнала. Уменьшение техпроцесса увеличивает производительность и уменьшает энергозатраты.

*2. Геометрическая модель физических ресурсов базовых информационных технологи***.** Модель физических ресурсов может быть представлена в виде куба (рисунок 1), который характеризует объем технологии, применяемой для реализации соответствующего информационного процесса. В этой модели ось ординат (S) отображает пространственные параметры технологии, примером которых могут служить плотность размещения оборудования, удаленность пользователей, плотность записей на носителях данных, размер транзисторов, площадь или объем технологических помещений, площадь фальшпола. Ось аппликат (F) отображает энергетические параметры технологии, такие как, например, киловатт-часы потребляемой энергии, выделяемая тепловая мощность или масса выделяемого углеводорода при выработке электроэнергии. Ось абсцисс (T) отображает временные параметры технологии, к числу которых относятся, например, времена сохранения, доставки и обработки данных, время распространения сигналов, время переключения элементов электрических схем и др., а также характеристики, обратные времени и имеющие смысл интенсивности наступления событий в единицу времени.

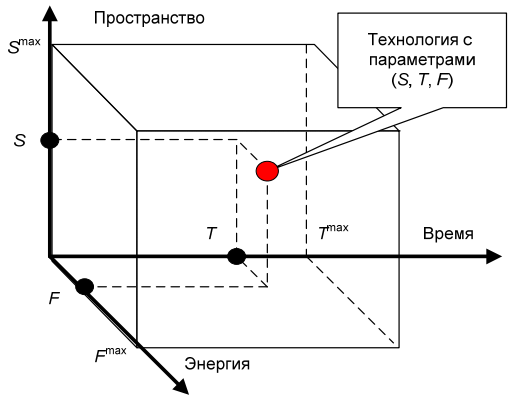


Рис. 1. Модель физических ресурсов информационных процессов

Точки, лежащие в пределах объема параллелепипеда и имеющие координаты 0≤S≤Smax, 0≤T≤Tmax, 0≤F≤Fmax, соответствуют некоторым уже реализованным или еще разрабатываемым технологиям.

Никакой информационный процесс нельзя реализовать, если отсутствует хотя бы один из технологических ресурсов, но у каждого из процессов существует главный ресурс, экономия которого наиболее существенно влияет на эффективность реализации информационного взаимодействия. Выявление главного ресурса для базовых информационных процессов основывается на особенности данных, представляющих собой последовательность материальных знаков.

Чем больше знаков в информационной последовательности, тем больший объем пространства нужен для их одновременного сохранения. Пространство, необходимое для сохранения данных, всегда пропорционально количеству знаков. Поэтому при любых временах хранения и доступной энергии для записи/чтения данных их нельзя сохранить, если отсутствует достаточный объем пространства. Главный технологический ресурс информационного процесса сохранения – это пространство, а технологическая характеристика – это плотность записи.

Таким образом, для выбора технологии сохранения пользователь должен задать:

– верхний уровень плотности записи или размер минимальной единицы хранения – S^{cox},
– нижний уровень допустимого времени гарантированного хранения – T^{cox},
– верхний уровень энергетического барьера – F^{cox}.

Это означает, что технология сохранения должна отвечать требованию:

$$S \le S^{cox},\ T \ge T^{cox},\ F \le F^{cox}.$$

Модель физических ресурсов процесса сохранения приведена на рисунке2.

Объем технологии сохранения увеличивается по мере увеличения времени жизни носителя данных, плотности записи и уменьшения энергии, затрачиваемой за время сохранения.

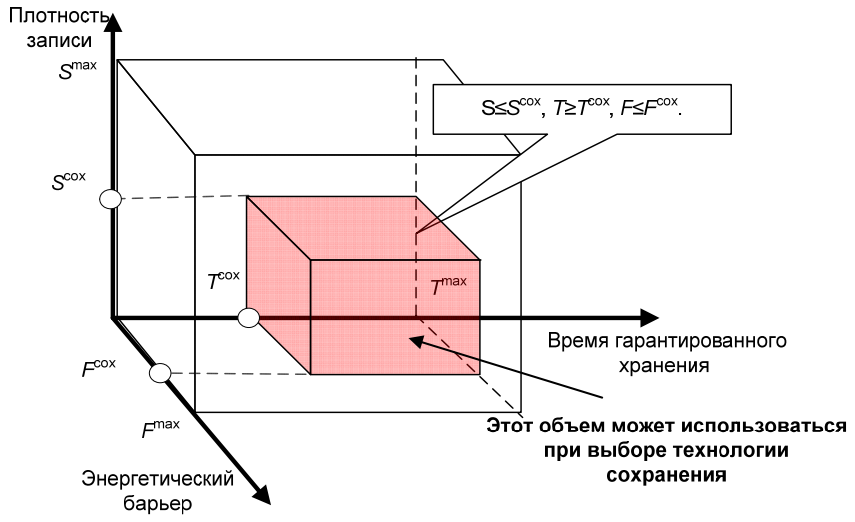


Рис. 2. Модель физических ресурсов процесса сохранения

Чем больше знаков в последовательности, тем большее время нужно для их последовательного перемещения в пространстве. При любых пространственных координатах коммуникантов и любых доступных объемах энергии данные нельзя распространить, если отсутствует время. Параллельное перемещение знаков информационной последовательности в пространстве не может быть реализовано на практике, а последовательное перемещение физических объектов не может произойти мгновенно. Поэтому время распространения всегда пропорционально количеству знаков в информационной последовательности. Главный технологический ресурс при распространении данных в пространстве – это время, а технологическая характеристика – время перемещения знака или сигнала.

Таким образом, для выбора технологии распространения пользователь должен задать:

– нижний уровень зоны охвата – S^{pac},
– верхний уровень допустимого времени доставки – T^{pac},
– верхний уровень отношения «сигнал/шум» – F^{pac}.

Это означает, что технология сохранения должна отвечать требованию:

$$S \ge S^{pac},\ T \le T^{pac},\ F \le F^{pac}.$$

Модель физических ресурсов процесса распространения приведена на рисунке3.

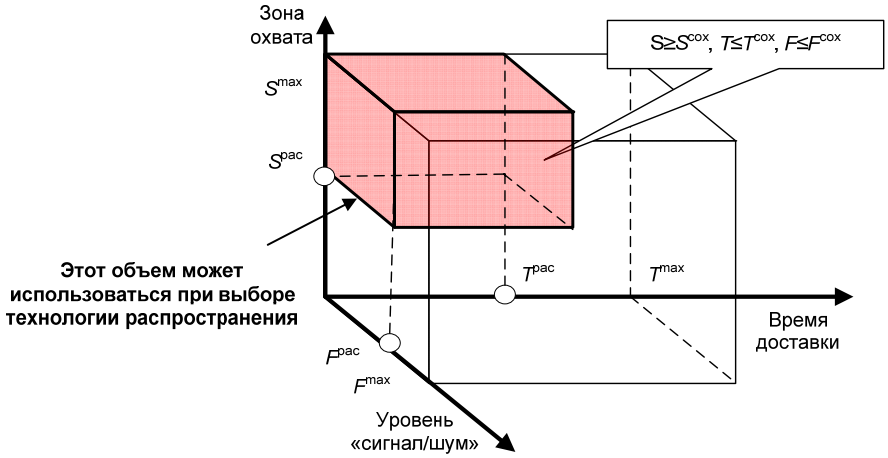


Рис. 3. Модель физических ресурсов процесса распространения

Объем технологии распространения увеличивается по мере увеличения территории охвата, уменьшения времени доставки данных и энергии, затрачиваемой за время доставки.

Обработка данных изменяет состав и (или) последовательность знаков информационной последовательности.Любые изменения структуры или формы физических объектов требуют энергии, которая выражает способность произвести нужные действия. При любых доступных объемах времени и любых размерах процессора данные нельзя обработать, если отсутствует энергия, которая пропорциональна количеству изменяемых знаков. Поэтому главный технологический ресурс при обработке данных – это энергия, а технологическая характеристика – энергозатраты на обработку одного бита данных.

Таким образом, Для выбора технологии обработки пользователь должен задать:

– верхний уровень техпроцесса – $S^{обр}$,
– верхний уровень времени переключения вычислительного элемента – $T^{обр}$,
– верхний уровень энергозатратна обработку одного бита – $F^{обр}$.

Технология сохранения должна отвечать требованию:

$$S \le S^{обр},\ T \le T^{обр},\ F \le F^{обр}.$$

Модель физических ресурсов процесса обработки приведена на рисунке4.

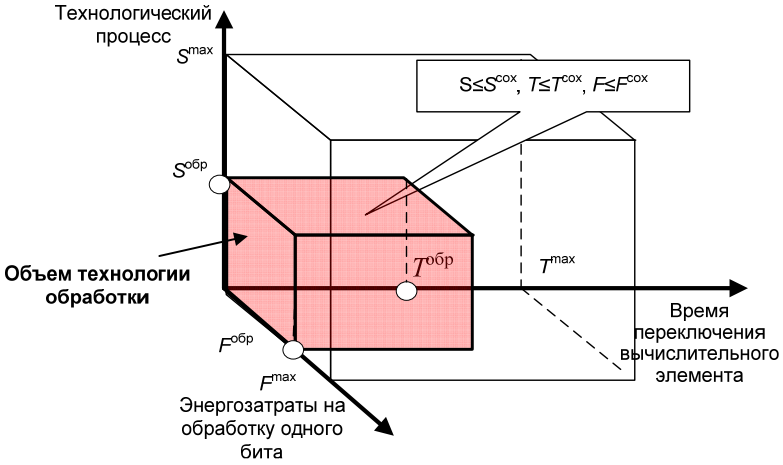


Рис. 4. Модель физических ресурсов процесса обработки

Объем технологии обработки увеличивается по мере уменьшения техпроцесса, времени обработки и энергии, затрачиваемой за время обработки.

На объемы технологических ресурсов мало влияют внешние условия реализации процессов информационного взаимодействия и поведение коммуникантов, поэтому их можно считать детерминированными.

Для сравнения достигнутых исходов выполнения информационных процессов и их отдельных этапов и фаз с исходами, которые являются желаемыми для коммуникантов, служат показатели эффективности. Значения этих показателей зависят не только от выбранных технологий, но и от поведения коммуникантов и объема данных взаимодействия, поэтому являются стохастическими. Дополнительное влияние на значения показателей оказывают коллизии, которые возникают при обращении нескольких коммуникантов к одним и тем же ресурсам[10]. Также отдельно следует рассматривать этапы доступа коммуникантов к среде взаимодействия и этапы преобразования данных.

Объемы физических ресурсов могут измеряться, как в удельных, так и в относительныхединицах и их значения являются важной характеристикой для выбора информационной технологии, реализующей соответствующий информационный процесс.

Заключение. Сегодня накоплено достаточное количество технологий хранения, распространения и обработки данных. Ресурсы для их реализации становятся все дороже. Перед специалистами встает задача выбора определенной технологии, с одной стороны, удовлетворяющей требованиям пользователей соответствующей услуги и, с другой стороны, обеспечивающей экономию физических ресурсов, необходимых для реализации процесса.

Классификация существующих технологий по различным параметрам позволяет упростить задачу выбора технологии, как специалистам, так и пользователям.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю.Ф., Колбанёв М.О. Технология инфокоммуникации. – Курск: Науком, 2011. – 260 с.
2. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Двухуровневая модель информационного взаимодействия// VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013.С 184
3. Шеннон К.Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – 830 с.
4. Колбанёв М.О., Яковлев С.А. Модели и методы оценки характеристик обработки информации в интеллектуальных сетях связи. – СПб.: СПбГУ, 2002. – 230 с.
5. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. О развитии технологии информационного общества// VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», Санкт-Петербург, 23-25 октября 2013.С 23
6. Советов Б.Я. Проблемы перехода к ноосферному образованию//4-я международная научно-практическая конференция «Ноосферное образование в Евразийском пространстве». – СПб., 2012 – 0,5 п.л.
7. Советов Б.Я., Колбанёв М.О., Татарникова Т.М.Оценка вероятности эрланговского старения информации//Информационно-управляющие системы, №6, 2013. С. 25-28.
8. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель балансировки нагрузки в вычислительном кластере центра обработки данных//Информационно-управляющие системы. 2012 № 3(58). С. 37-41.
9. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И. Модель обработки клиентских запросов//Телекоммуникации. 2013 №9. С. 42-48.
10. Верзун Н.А. Множественный доступ в информационных системах. Учебное пособие. СПб.: СПбГУТ, 2007. 92 с.

УДК 378.147; 004.9

РОЛЬ И МЕСТО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В НАПРАВЛЕНИИ ПОДГОТОВКИ 080101.65 «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ»

Коршунов Игорь Львович, Суворова Ольга Викторовна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mails: kil53@mail.ru, it107@mail.ru.

Аннотация: Предлагается подход к изучению дисциплин, связанных с информационными технологиямии информационной безопасностьюпонаправлению обучения 080101.65 «Экономическая безопасность» что позволит специалистамовладеть компетенциям, отвечающих требованиям Федерального государственного образовательного стандарта.

Ключевые слова: *учебный процесс; образовательная программа; экономическая безопасность; компетенция, специалист; информационная технология; информационная безопасность.*

THE ROLE AND PLACE OF INFORMATION TECHNOLOGIES IN THE FIELD OF TRAINING 080101.65 "ECONOMIC SECURITY"

Korshunov Igor, Suvorova Olga,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mails: kil53@mail.ru, it107@mail.ru.

Abstract: A proposed approach to studying subjects related to information technologies and information security by field of study 080101.65 "Economic security" which will allow specialists to master the competencies that meet the requirements of the state educational standard..

Keywords: *the educational process; educational programme; economic security; competence, specialist; information technology; information security.*

В соответствии с Федеральным государственным образовательным стандартом (ФГОС) специалист в области экономической безопасности готовится к информационно-аналитической деятельности. Он должен уметь решать целый ряд задач, связанных с поиском и оценкой истинности информации, имеющей значение для обеспечения экономической безопасности; с моделированием экономических процессов в целях анализа и прогнозирования угроз экономической безопасности; с информационно-аналитическим обеспечением предупреждения и выявления экономических рисков и угроз экономической безопасности.

Среди многочисленных компетенций (общекультурных и профессиональных), которыми должен обладать специалист, необходимо отметить следующие: способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике, автоматизированные рабочие места, проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач; способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор; способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в учетно-отчетной документации, использовать полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности.

Анализ приведенных требований ФГОС позволяет констатировать, что специалист в области экономической безопасности должен хорошо знать теоретические основы информационных технологий, уметь применять их в профессиональной деятельности и владеть методами и средствами информационной безопасности. Для достижения этих целей в базовой части математического и естественнонаучногоцикла примерной основной образовательной программы имеется дисциплина «Информационные системы в экономике». К сожалению, она не позволит в полной мере подготовить специалиста, обладающего приведенными выше компетенциями.

Знакомство с основными образовательными программами данного направления ряда вузов страны показало, что отсутствует единый подход в понимании значения и роли информационных технологий в подготовке специалистов данного направления. В некоторых вузах кроме базовой дисциплины «Информационные технологии в экономике» присутствует только дисциплина «Информатика» (Вятский государственный гуманитарный университет). В других вузах в вариативную часть (дисциплины по выбору студента) включены несколько дисциплин, имеющих информационную направленность, например: «Автоматизированные системы учета, анализа и аудита» и «Безопасность электронного документооборота» (Тамбовский государственный университет);

«Безопасность систем БД» и «Безопасность ОС» (Томский государственный университет систем управления и радиоэлектроники); «Офисные информационные технологии в деятельности экономистов» (Московская академия экономики и права) и др.

Для подготовки специалиста, отвечающего требованиям ФГОС в области информационных технологий, предлагается включить в вариативную часть математического и естественнонаучного цикла дисциплину «Информационная безопасность». Данная дисциплина имеется в основных образовательных программах Российской академии народного хозяйства и государственной службы при Президенте РФ, Тамбовском государственном университете, Южно-Уральском институте управления и экономики.

В этом случае в рамках дисциплины «Информационные системы в экономике» целесообразно рассматривать [1],[2]базовые информационные процессы, базовые информационные технологии и информационные системы, реализующие информационные технологии в экономике. Вторую дисциплину «Информационная безопасность» следует посвятить изучению информационных технологий защиты информации, применяемых в профессиональной сфере специалистов по экономической безопасности.

Если вернуться к задачам, которые должен уметь решать выпускник данного направления, перечисленным в первом абзаце данной статьи, то можно предположить, что дисциплина «Информационные технологии в экономике» позволит подготовить выпускника к решению первых двух задач. Дисциплина «Информационная безопасность» должна подготовить студента к решению второй и третей задач. Процесс изучения дисциплины «Информационные технологии в экономике» должен быть нацелен на формирование у студента всех трех компетенций, перечисленных в начале статьи. Целью дисциплины «Информационная безопасность» следует считать формирование у студента компетенции, связанной со способностью использовать полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности.

Для достижения указанной цели предлагается следующая структура и содержание дисциплины «Информационные технологии в экономике». Целесообразно весь материал дисциплины разбить на четыре темы: Информация и ее роль в экономике; Информационные процессы; Информационные технологии; Информационные системы.

Содержанием темы «Информация и ее роль в экономике» могут быть: информация и ее свойства; формы представления информации; количественные и качественные характеристики информации; классификация информации, используемой в экономике.

В теме «Информационные процессы» рекомендуется рассматривать вопросы, связанные с определением понятия информационный процесс, его основными характеристиками, его концептуальной моделью. Далее целесообразно подробнее рассмотреть часто используемые в экономике базовые информационные процессы: извлечения информации, транспортирования информации[3,4], обработки информации, хранения информации, представления и использования информации.

Изучение темы «Информационные технологии» логично начать с определения понятия информационная технология, роли информационных технологий в развитии экономики и общества. Затем рекомендуется рассмотреть некоторые виды информационных технологий, широко используемых в экономике: организационного управления; инфокоммуникационные; геоинформационные; мультимедиа; искусственного интеллекта. Рассмотрение темы «Информационные системы» целесообразно начать с определения понятия информационная система, его связи с понятиями информационный процесс и информационная технология. Структуру и описание базовой информационной системы логично осуществить на концептуальном, логическом и физическом уровнях. Более подробно рекомендуется рассмотреть корпоративные информационные системы: их роль и место в экономике; задачи, функции и структура этих систем; программное и техническое обеспечение функционирования подобных систем.

На практические занятия по дисциплине «Информационные технологии в экономике» рекомендуется вынести следующие темы: Поиск и оценка экономической информации, Моделирование экономических процессов, Методы, способы и средства работы с экономической информацией, Инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации, Применение в профессиональной деятельности автоматизированных информационных систем, Анализ и интерпретация финансовой, бухгалтерской и иной информации с использованием средств автоматизации.

Дисциплина «Информационная безопасность» должна базироваться на знаниях, полученных студентами при изучении дисциплины «Информационные технологии в экономике». Для достижения цели и задач дисциплины «Информационная безопасность» рекомендуется включить в нее для изучения следующие темы: Концепция информационной безопасности, Внешние и внутренние угрозы экономической безопасности, Технические каналы утечки информации, Методы и средства защиты информации от утечки по техническим каналам, Информационно-аналитическое обеспечение предупреждения и выявления угроз экономической безопасности.

В теме «Концепция информационной безопасности» целесообразно рассмотреть вопросы, связанные с содержанием и структурой основных понятий и терминов в области технической защиты информации[5]; с основополагающими для информационной безопасности категориями: доступность, целостность и конфиденциальность информации; с требованиями, предъявляемыми к защите информации. Рекомендуется подробно рассмотреть концептуальную модель безопасности информации как основу создания системы защиты информации в организации.

Тема «Внешние и внутренние угрозы экономической безопасности» предполагает знакомство студентов с особенностями современных информационных систем как объекта защиты информации. Целесообразно далее рассмотреть классификацию угроз безопасности информации, дать подробную характеристику каждому виду угроз. Рекомендуется также рассмотреть типовые модели угроз безопасности экономической информации. Затем целесообразно ознакомить студентов с основными классами атак, осуществляемых на корпоративные информационные системы, и с методами оценки опасности угроз.

В теме «Технические каналы утечки информации» предлагается рассмотреть:причины и физические явления, порождающие технические каналы утечки информации при эксплуатации информационной системы; модель технического канала утечки информации; классификацию технических каналов утечки информации.

Изучение темы «Методы и средства защиты информации от утечки по техническим каналам» предполагает знакомство студентов с организацией и реализацией мероприятий по защите информации от утечки по различным техническим каналам. В этой же теме рекомендуется рассмотреть вопросы, связанные с особенностями программно-математического воздействия вредоносных программ и защиты от них в корпоративных информационных системах.

Последняя тема «Информационно-аналитическое обеспечение предупреждения и выявления угроз экономической безопасности» предполагает применение студентами полученных при изучении предыдущих тем знаний в профессиональной деятельности, связанной с обеспечением защиты экономической информации от внешних и внутренних угроз[6]. Рекомендуется сделать упор на изучение системподдержки принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности [7]. Для практических занятий по дисциплине «Информационная безопасность» предлагаются следующие темы: Инструментальные средства защиты информации от утечки по техническим каналам, Методы и средства защиты от программно-математического воздействия на экономическую информацию, Анализ и прогнозирование угроз экономической безопасности, Информационно-аналитическое обеспечение экономической безопасности, Инструментальные средства системы поддержки принятия решений по экономической безопасности.

Авторы считают, что предлагаемый подход к изучению студентами направления 080101.65 «Экономическая безопасность» современных информационных технологий и информационной безопасности позволит подготовить специалистов, отвечающих требованиям Федерального государственного образовательного стандарта (обладающих соответствующими компетенциями) в части, касающейся информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Цехановский В.В.Информационные технологии: Учеб.для вузов/ - 3-е изд., стер. – М.: Высш. шк., 2006. – 263 с.
2. Трофимов В.В., Ильина О.П., Трофимова Е.В., Князев В.И., Приходько А.П. Информационные системы и технологии в экономике и управлении: Учеб.для вузов/- 4-е изд., под ред. В.В.Трофимова. – СПб.: Издательство: Юрайт, ИД Юрайт, 2013. 376с.
3. Колбанёв М.О., Татарникова Т.М., Воробьёв А.И.Модель обработки клиентских запросов//Телекоммуникации, №9, 2013. С. 42-48.
4. Богатырев В.А., Богатырев С.В., Богатырев А.В.Функциональная надежность вычислительных систем с перераспределением запросов // Изв. вузов. Приборостроение. 2012. Т. 55. № 10. С. 53–57.
5. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность, №1, 2014. С. 69-77.
6. Левкин И.М.Теория и практика информационно-аналитической работы. – Курск, НАУКОМ, 2014.
7. Пуха Г.П.Методология формирования и реализации систем интеллектуальной поддержки принятия решений. / Г.П. Пуха. – СПб.: СМИО-Пресс, 2012. –337 с.

УДК 351.863

ВНЕШНЕЭКОНОМИЧЕСКАЯ ЭКСПАНСИЯ: ПРИЗНАКИ СОСТОЯНИЯ

Левкина Светлана Вячеславовна[1], Микадзе Сергей Юрьевич[2],
[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, д. 49,
[2]Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mail: lev.kin@mail.ru.

Аннотация: В статье уточняется понятие внешнеэкономической экспансии как комплекса согласованных и взаимосвязанных по целям, задачам, месту и времени мероприятий. На этой основе

формируются основные элементы внешнеэкономической экспансии: начальные, конечные и фиктивное состояния, мероприятия и их информационные (идентификационные) признаки. На их основе строится информационная (информационно-признаковая) модель (фрейм-сценарий). Описывается механизм работы с моделью в интересах решения основных задач экономического мониторинга.

Ключевые слова: *внешнеэкономическая экспансия, экономическая угроза, мероприятия, состояния, информационные (идентификационные) признаки, информационная (информационно-признаковая) модель, фрейм-сценарий, субфрейм, задачи экономического мониторинга.*

FOREIGN ECONOMIC EXPANSION: SIGNS OF THE CONDITION

Levkina Svetlana[1], Mikadze Sergey[2],
[1]St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverkskiy av. 49,
[2]Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: lev.kin@mail.ru.

Abstract: In this article clarifies the concept of foreign economic expansion as a set of coherent and interrelated goals, tasks, time and place of events. On this basis are formed the main elements of the international economic expansion: the initial, final and fictitious status, activities and their information (identification) signs. They form the basis for information (information-attribute) model (frame-scenario). Describe the mechanism of work with the model for the solution of the major tasks of economic monitoring.

Keywords: *foreign trade expansion; economic threat; activities; status information (identification) signs; information (information- attribute) model; the frame script; the subframe script; the tasks of economic monitoring.*

Внешнеэкономическая экспансия является особой формой экономической угрозы. Это связано: во-первых, с масштабностью целей, которые она преследует (расширение сферы экономического влияния, вытеснение других стран, фирм, захват рынков, приобретение ресурсных источников) [1]; во-вторых, с масштабностью и разнообразием методов используемых для достижения этих целей.

Стимулом к экономической экспансии служит погоня за прибылью, которая протекает в жёсткой конкурентной борьбе за рынки сбыта, источники сырья, выгодные сферы приложения капитала. В современных условиях экономическая экспансия приобретает форму поисков и борьбы за ниши в международном разделении труда, на мировых рынках. Выигравшей в ней стороной становится та страна, отрасль, фирма, которая впишется в такую нишу, наладив производство конкурентоспособной продукции [2].

Анализ существующих подходов к экспликации внешнеэкономической экспансии свидетельствует, что они акцентируют внимание только на цели, в интересах которых такая экспансия осуществляется, оставляя за рамками сам процесс ее проведения. Это:

– во-первых, затрудняет комплексный анализ процессов внешнеэкономической экспансии в различных условия внешне политической и внешне экономической обстановки;

– во-вторых, не позволяет строить адекватные математические модели процесса внешнеэкономической экспансии, проводить расчеты и делать научно обоснованные прогнозы.

С целью устранению этих недостатков подойдем к экспликации внешнеэкономической экспансии по-новому и будем понимать ее как комплекс согласованных и взаимосвязанных по целям, задачам, месту и времени мероприятий, проводимых по единому замыслу и плану политическими и экономическими структурами зарубежного государства (коалицией государств) с целью расширения сферы экономического влияния, вытеснения других стран, фирм, захвата рынков, приобретения ресурсных источников.

Данное определение предполагает для изучения степени опасности внешнеэкономической экспансии выполнение следующих обязательных действий:

– определение основных конечных состояний, в которые экономическая система может перейти в результате внешнеэкономической экспансии;

– формирование перечня основных мероприятий (событий), которые проводятся для достижения целей внешнеэкономической экспансии;

– выявление взаимосвязей между этими мероприятиями.

Конечными состояниями экономической системы могут быть:

S1 – изменение направленности экономических взглядов научного сообщества Российской Федерации на неоклассические экономические теории;

S2 – смещение внешней торговли Российской Федерации с посреднических услуг и готовой продукции на сырьевые отрасли;

S3 – контроль над ключевыми отраслями промышленности;

S4 – захват финансово-кредитной системы Российской Федерации.

Переход экономической системы из начального состояния S0 (начало активизации экономической экспансии) в одно или несколько конечных состояний осуществляется через реализацию ряда взаимосвязанных мероприятий (событий). Множество этих мероприятий M_j , $j = \overline{1,32}$ сформировано путем анализа основных процессов, осуществляемых при внешнеэкономической экспансии [3-9]. В их число включены:

M1 - включение в свои зоны ответственности территории государства;

M2 - разработка новой “привлекательной” экономической теории;

M3 - выработка стратегии действий транснациональных банков;

M4 - выработка стратегии действий транснациональных компаний;

M5 - ужесточение контроля (запрет) над экспортом современных технологий;

M6 – проведение “цветных революций” в сопредельных и дружественных странах;

M7 - развитие одного из регионов страны-соперницы на значительно высший, чем в других регионах, уровень за незначительное время;

M8 - ухудшение экономики наименее развитого региона;

M9 – запрет на экспорт ряда товаров (технологий);

M10 - борьба с терроризмом;

M11 - принятие решения о выводе из развитых стран "грязных" технологий;

M12 - введение экономических санкций;

M13 - создание недружественного экономического окружения;

M14 - сбыт залежалых и вредных лекарств;

M15 - подготовка кадров в рамках принятой теории для работы в стране – объекте экспансии;

M16 - скупка акций наиболее крупных банков и фирм;

M17 - навязывание кабальных финансовых договоров;

M18 - участие во внешнеэкономической экспансии США ряда международных организаций. Речь идет о таких международных государственных кредитных учреждениях, которые осуществляют вывоз капитала в виде займов;

M19 - блокирование альтернативных экономических проектов;

M20 - усиление разбалансирования в экономическом развитии регионов (субъектов федерации);

M21 - консервация однотипной сырьевой ориентации экономики и экспорта;

M22 - давление долговыми обязательствами, привязки экономики страны к донорству и использования этой "привычки";

M23 - организация полной экономической блокады;

M24 – создание промышленных трудностей;

M25 - пропаганда “правильного” образа жизни;

M26 - продвижение на ключевые государственные посты коллаборационистов;

M27 - создание ТНК широкой сети дочерних компаний, филиалов, участий в совместных предприятиях;

M28 - рост социальной напряженности;

M29 - развитие отдельных предприятий и отраслей, преимущественно ориентированных на внешний рынок и на иностранный капитал;

M30 – организация “цветной” революции в стране (РФ);

M31 - снижение научно-технического и производственного потенциала;

M32 - создание финансовых трудностей.

Выявлении связей между перечисленными мероприятиями позволяет создать фрейм-сценарий внешнеэкономической экспансии [10]. Сценарий представляет собой последовательность действий, которые описывают часто встречающиеся ситуации. В этой последовательности действий используется принцип каузальной связи, т. е. результатом каждого действия являются условия, при которых может произойти следующее действие.

К основным особенностям построения фрейм-сценария (сетевой информационно-признаковой модели) внешнеэкономической экспансии в отношении РФ (рисунок 1) относятся:

1. Каждое мероприятие (событие) M_s $s = \overline{1,32}$, представляющее собой терминал (узел) фрейма может быть представлено иерархическим взвешенным графом типа “корневое дерево”, построенным при помощи информационных (идентификационных) признаков a_i, событий и угроз (события и угрозы в свою очередь также являются информационными (идентификационными) признаками только более высокого уровня). Перечень информационных признаков (априорный словарь) формируется путем изучения информационного пространства [11,12]. Пример такого графа для мероприятия (угрозы) M_{13} приведен на рисунке 2.

2. Наступление мероприятия (события) соответствует логическим операциям ***И/ИЛИ*** и фиксируется в случае превышения индикатором вершины соответствующего иерархического взвешенного графа типа “корневое дерево” $I_{i,v}$ (a_h) заданного порогового значения.

3. Предложенный фрейм-сценарий не должен иметь пустых узлов. Это означает, что любое мероприятие (событие) обязательно должно приводить либо к началу промежуточного фрейма (субфрейма (ситуации)), либо к одному из конечных состояний.

4. Подобный фрейм-сценарий должен завершаться одним фиктивным состоянием, означающим степень (вероятность) достижения цели. Это состояние является конечным узлом фрейм-сценария, входными элементами которого являются сформированные конечные состояния $S_1, S_2, \ldots$

5. Каждый субфрейм (кроме начальных $S_0 - M_r$, $r \in \{1,2,3,4,5,6,7,8,9,10,11,14\}$) представляет собой иерархический взвешенный граф типа “корневое дерево” состоящий из узла и непосредственно входящих в него мероприятий.

Перечисленные особенности одновременно являются требованиями к построению аналогичных фрейм-сценариев (сетевых информационно-признаковых моделей).

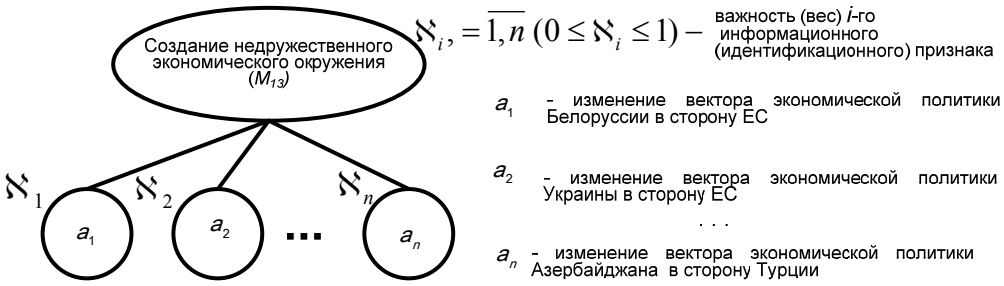


Рис. 2. Информационная (информационно-признаковая) модель мероприятия “Создание недружественного экономического окружения” в виде иерархического взвешенного графа типа “корневое дерево” (фрагмент)

Предложенная модель позволяет решать следующие задачи.

1. Задача определения по проявившимся информационным (идентификационным) признакам вероятности наступления соответствующих мероприятий и прогнозирование проведения связанных с ним последующих мероприятий.

При обнаружении информационных (идентификационных) признаков $a_1, a_2, \ldots, a_h$, непосредственно принадлежащих мероприятию M_s вероятность его зарождения $I_{M_s}(a_1, a_2, \ldots, a_h)$ может быть определена по формуле [11]:

$$I_{M_s}(a_1, a_2, \ldots, a_h) = 1 - \left(1 - \prod_i \left(1 - \aleph_i I_{M_s}(a_i)\right)\right), . \quad (1)$$

Мероприятие будем считать завершенным, если его индикатор превышает заданное пороговое значение:

$$I_{M_s}(a_1, a_2, \ldots, a_h) \ge I^*. \quad (2)$$

Результаты решения этой задачи могут применяться для определения вероятности связанного с мероприятием M_s следующего по времени проявления мероприятия. В этом случае вероятность его проведения может быть рассчитана по соответствующему субфрейму, тем же методом, но при этом роль исходных данных (информационных (идентификационных) признаков) будут играть вероятности проведения входящих в узел M_h, $h>s$ ранее проявившихся мероприятий. На рисунке 3 приведен пример для $M_s = M_{23}$, а ранее проявившиеся мероприятия – $M_5, M_9, M_{12}, M_{13}, M_{19}$.

В связи с тем, что мероприятие M_s в свою очередь является подчиненным элементом следующего узла (субфрейма) – например, каузальная связь M_{23} - M_{31} на рисунке 4, вероятность его проведения будет являться исходными данными для прогнозирования (расчета вероятности проведения) этого следующего узла.

2. Задача определения степени развития внешнеэкономической экспансии. Одной из особенностей внешнеэкономической экспансии является то, что, не смотря на наличие пространственно-временной каузальной зависимости проводимых мероприятий, отдельные информационные (идентификационные) признаки поздних мероприятий могут проявляться раньше, чем предыдущих мероприятий. Например, информационные (идентификационные) признаки мероприятия М29 (развитие отдельных предприятий и отраслей, преимущественно ориентированных на внешний рынок и на иностранный капитал) могут появиться раньше, чем информационные (идентификационные) признаки мероприятия М15 (подготовка кадров в рамках принятой теории для работы в стране – объекте экспансии). Однако в полном объеме мероприятие М29 завершиться раньше, чем завершиться мероприятие М15 не может. Завершением мероприятия Ms, как было указано выше, является превышение его индикатора заданного порогового значения. Поэтому степень развития внешнеэкономической экспансии будем определять временем завершения входящих в фрейм-сценарий мероприятий.

Рис. 1. Информационно-признаковая сетевая модель внешнеэкономической экспансии

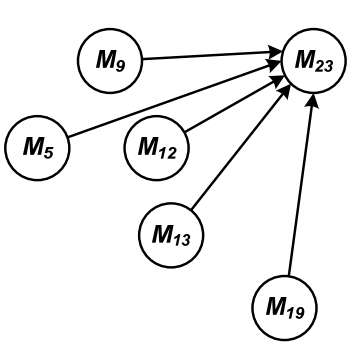


Рис. 3. Субфрейм узла M_{23}

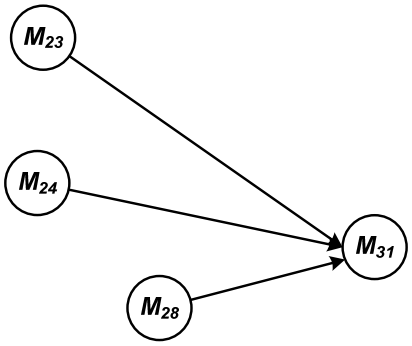


Рис. 4. Субфрейм узла M_{31}

3. Задача оценки эффективности ответных действий при принятии решения на противодействие тому или иному мероприятию и их совокупностям. Меры противодействия мероприятиям внешнеэкономической экспансии снижают вероятность их реализации. Это проявляется в исчезновении ряда ключевых информационных (идентификационных) признаков. В зависимости от числа ликвидированных признаков будет получено то или иное значение вероятности проведения соответствующих мероприятий. Наиболее эффективным будет считаться тот вариант ответных действий Ω_k, который обеспечит максимальное снижение вероятности проведения мероприятия:

$$I_{i,v}(a_1, a_2, ..., a_s) \xrightarrow[\Omega]{} \min,$$

где Ω - множество вариантов ответных действий.

СПИСОК ЛИТЕРАТУРЫ

1. Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б. Современный экономический словарь. - 5-е изд., перераб. и доп. — М.: ИНФРА-М, 2006.
2. Экспансия. - http://murzim.ru/nauka/jekonomika/22158-ekspansiya.html.
3. Моро-Дефарж Ф. Введение в геополитику. - http://www.democracy.ru/library/misk/introduction_in_geopolitics/;
4. Экономическая экспансия и экономическая независимость. -
5. http://duheconomy.ucoz.org/publ/ehkonomicheskaja_ehkspansija_i_ehkonomicheskaja_nezavisimost/1-1-0-8;
6. Экономический цикл и кредитная экспансия. -
7. http://liberty-belarus.info/Ekonomicheskaya-teoriya/Ekonomicheskiy-tsikl-i-kreditnaya-ekspansiya.html.;
1. Голубович В.И. Экономическая история зарубежных стран. -
8. http://uchebnik-besplatno.com/uchebnik-istoriya-ekonomiki/vneshneekonomicheskaya-ekspansiya-amerikanskogo.html;
9. Внешнеэкономическая экспансия американского капитала и начало борьбы за колонии. - http://econbez.narod.ru/1security/2articles/2.htm.;
10. Американское нашествие. - http://konspekts.ru/ekonomika-2/amerikanskoe-nashestvie/.;
11. Лисицкий В. Экспансия США и крепнущая Россия. - http://www.yermak.com.ua/txt/pol/art_ekspansion.html.;
12. Экономическая война за новый мировой порядок. - http://topwar.ru/23619-ekonomicheskaya-voyna-za-novyy-mirovoy-poryadok.html.
13. Шенк Р., Абельсон Р. Сценарий, планы и знание.— В кн.: Тр. IV Междунар. объед. конф. по ИИ. М., 1975.
14. Левкин И.М. Теория и практика информационно-аналитической работы. – Курск: НАУКОМ, 2011.
15. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Оценка вероятности эрланговского старения информации//Информационно-управляющие системы, №6, 2013. С. 25-28.

УДК 004.93

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Маркелов Константин Сергеевич, Нечаев Валентин Викторович,
Московский государственный технический университет радиотехники, электроники и автоматики (МГТУ МИРЭА),
Россия, Москва, Проспект Вернадского, д. 78,
e-mail: kosmar89@mail.ru,nechaev@mirea.ru.

Аннотация: Рассматривается одно из активно развивающихся направлений информатики – биометрия с прикладной ориентацией на применения в рамках социально-экономической безопасности. Введено понятие и построена модель комплексной биометрической информационной технологии (БМИТ), состоящей из четырёх этапов, приводится описание каждого этапа. Рассматриваются положительные и отрицательные стороны применения БМИТ для решения задач социальной и экономической безопасности.

Ключевые слова: *безопасность; информационная безопасность; биометрические информационные технологии (БМИТ); биологическая информационная технология (БИТ); информационно-измерительная технология (ИИТ); компьютерная информационная технология (КИТ); технология идентификации индивида (ТИИ).*

BIOMETRIC TECHNOLOGY AS A FACTOR OF SOCIO-ECONOMIC SECURITY

Markelov Konstantin, Nechaev Valentin,
The Moscow state technical university of radio engineering, electronics and automatics (MGTU MIREA),
Russia, Moscow, Vernadsky Avenue 78,
e-mails: kosmar89@mail.ru,nechaev@mirea.ru.

Abstract:.Is considered one of the rapidly developing areas of computer science - Applied Biometrics with a focus on applications in the framework of socio-economic security. And introduced the concept of a model of an integrated biometric information technology (BMIT), consisting of four stages, a description of each stage.

We consider the positive and negative aspects of using BMIT for solving problems of social and economic security.

Keywords: *security, information security; biometric information technology (BMIT); biological information technology (BIT); measuring and information technology (IIT); computer information technology (CIT); the technology of identification of the individual (TII).*

Введение. XXI векхарактеризуется большими изменениями в различных сферах жизни общества. Прежде всего - это политические, социальные, экономические, технические изменения. Широкое развитие получила вычислительная техника, появились новые направления,методы и средства деятельности, а главное - всё это стало необходимым для повседневной жизни. Появилась настоятельная необходимость надёжного, достоверного и оперативного контролядоступа на определенные объекты. В обеспечении идентификации и подтверждении личности в рамках электронного правительства, при пользовании электронными социальными, медицинскими услугами, в обеспечении контроля сетевого доступа и идентификации клиентов при работе с финансовыми учреждениями, в обеспечении учёта и контроля перемещения по стране иностранных граждан и т.п.

На современном этапе развития России без широкого внедрения новых (электронных) технологий достаточно сложно представить строгую регистрацию и учёт населения. Возросли миграционные потоки из стран ближнего и дальнего зарубежья. Получить достоверные персональные данные о том или ином человеке не всегда представляется возможным. Именно создание баз данных с хранением персональных данных и идентификация по этим даннымконкретных людей даёт возможность создать эффективную и строгую систему регистрации населения.

Существует множество сфер и областей жизнедеятельности человека, в которых необходимо подтвердить или идентифицировать личность. Для решения такого рода задач находят широкое применение методы биометрической идентификации личности – биометрия [1].

Для успешного решения перечисленных выше задач особоезначение приобретают используемые методы, модели, технологии и средства, используемые для обеспечения безопасности. Представляется,что наиболее эффективно было бы использованиеуниверсальной технологии, включающую в себя человека, а такжемодели, алгоритмы и программы, реализуемые в виде некоторыхсистемных приложений.Совокупность биометрических методов¸ формальных моделей, алгоритмов, средств обработки и хранения результатов составляют технологию, определяемую как биометрическую.

Идентификация личности по биометрическим данным используется для решения определённого спектра задач и находит широкое применение в различных прикладных системах идентификации, например таких, как: социальные, экономические, финансовые, коммерческие, миграционные, криминалистические, а также в системах специального назначения.

В настоящее время достаточно чётко определились и области применения биометрических информационных технологий. Приведём некоторые из них.

Системы гражданской идентификации включают в себя:

– паспорта, электронные универсальные карты;
– национальные идентификационные карты граждан;
– регистрацию избирателей;
– регистрацию для социальных программ;
– иммиграционную регистрацию, визы;
– контроль и регулирование миграционных потоков;
– идентификацию сотрудников государственных учреждений;
– различные виды личных документов, использование которых даёт владельцу возможность доступа к определённым возможностям;
– защита от несанкционированного доступа к разнообразным видам ресурсов.

Рис. 1 - Системы гражданской идентификации

Криминалистические системы идентификации включают в себя:

– находится ли данный гражданин в розыске;
– проверка судимости;
– регистрацию заключенных/контроль доступа;
– мобильные и удаленные приложения;
– обработку отпечатков пальцев и иных следов, полученных с мест преступления.

Рис. 2 – Криминалистические системы идентификации

Крупномасштабные коммерческие приложения включают в себя:
– доступ к электронным ресурсам, web ресурсам электронную коммерцию;
– доступ для пользователей, сотрудников;
– финансовые сервисы, проверку оплаты, банки «онлайн»;
– доступ в помещения, здания, секретные и закрытые объекты.

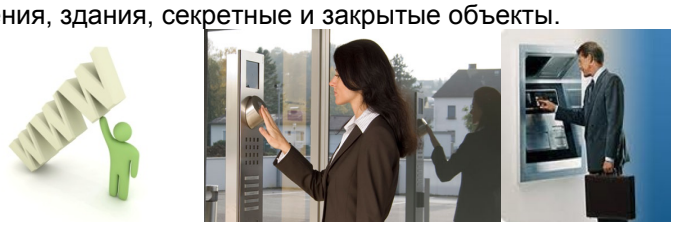


Рис. 3 – Крупномасштабные коммерческие приложения

Биометрические информационные технологии

Любая система идентификации должна формироваться по определенным технологиям. В рассматриваемом случае такими технологиями является биометрические информационные технологии (БМИТ). БМИТ – это развивающееся комплексное научно-практическое направление в структуре информатики. Целевое назначение БМИТ – идентификация личности человека на основе неотъемлемых от его организма предметов, свойств и т.п. [1], [2].

Комплексная БМИТ основана на органическом сочетании четырёх этапов информационной деятельности, каждый из которых характеризуется своей технологией, а в совокупности составляют комплексную технологию, направленную на достижение цели по идентификации личности в различного родах задач по распознаванию, идентификации, верификации(рис. 4).

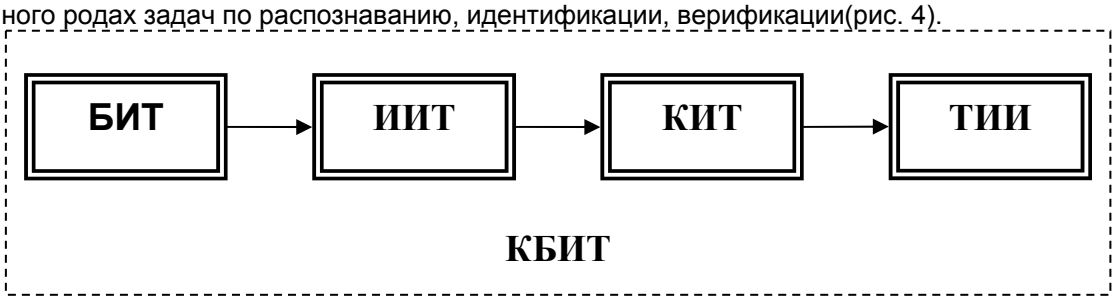


Рис. 4 – Схема концептуальной модели комплексной биометрической информационной технологии идентификации индивида

1. Биологическая информационная технология (БИТ). Первый этап - связан с организмом идентифицируемого человека. На этом этапе определяются те уникальные, неотъемлемые от организма человека предметы, которые дают возможность при определённых условиях решать задачу идентификации личности человека. Такие предметы определим как биологические идентификаторы (БИ).

2. Информационно-измерительная технология (ИИТ). Второй этап ориентирован на получение (съём) и первичную обработку информации с выделенных на первом этапе БИ. Для формирования такой информации используются методы или способы, технологии и средства информационно-измерительной техники.

3. Компьютерная информационная технология (КИТ). На третьем этапе осуществляется компьютерная обработка информации, полученной на втором этапе.При этом используются математические и иныеметоды, адекватные решаемым задачам. Следует отметить, что любой из методов биометрической идентификации должен обеспечивать возможность выделения уникальных особенностей БИ и представления их в форме совокупности унифицированных данных, которые называются биометрическим информационным портретом (БМИП) индивида.

4. Технология идентификации индивида (ТИИ). На четвёртом этапе осуществляется непосредственная реализация процесса идентификации. Далее на основе определённых методов и алгоритмов осуществляется поиск в банке биометрических данных (ББМД) прототипа – такого же или наиболее близкого БМИП. Найденные в ББМД прототипы сравниваютсяс оригинальными БМИП.По

результатам сравнения производится оценка и принятие решения. Если в ББМД не найдено его оригинала БМИП, то он рассматривается как новый и заносится по определённой методике и технологии в ББМД.

Введение в практику решения перечисленных выше задач на основе комплексной БМИТ даёт возможность расписать любой биометрический метод идентификации в рамках четырёх этапов в форме соответствующих задач. Каждая из задач позволяет выделить некоторую модель решения по идентификации личности. Модель решения в свою очередь позволит создать приложение или программное обеспечение по идентификации личности, отвечающее конкретным требованиям по безопасности. Например, где-то будет достаточно использование одного биометрического параметра, такого как отпечаток пальца, а где-то, в более сложных системах, а также в системах с более высокой степенью безопасности, потребуется использование нескольких биометрических параметров - комплексов, например, отпечатка пальца и сетчатки глаза.

Практическое применение БМИТ в задачах идентификации и верификации даёт возможность использовать совокупность положительных моментов, например, по сравнению с использованием привычных паролей и ПИН кодов. При использовании БМИТ:

– повышается степень защиты информации о человеке;
– повышается уровень идентификации человека в любых сферах применения (визы, оплата, социальные услуги и т.п.);
– нет необходимости носить идентификационные карты и придумывать идентификаторы для людей;
– повышается уровень безопасности охраняемых территорий;
– повышается удобство допуска на охраняемую территорию;
– повышается надёжность данных учёта рабочего времени на предприятии;
– появляется возможность подсчёта количества людей в местах общественного пользования;
– появляется возможность выявления преступных элементов, снижается угрозы беспорядков и террористических актов;
– повышается защита транзакций и удобство пользователей с банковскими операциями;
– повышается ответственность персонала на рабочих местах
– экономия времени при идентификации и т.п.

Однако, БМИТприсущи и определённыенедостатки. Прежде всего, это организационно-технические проблемы: нестабильность распознавания, дополнительные требования к оборудованию, возможные проблемы с обслуживанием; правовые проблемы: нет достаточно полной законодательной защиты по направлениям биометрии;этические проблемы: ограничение свобод граждан;проблемы риска и ответственности, как следствие - использование консервативных технологий;психологические проблемы: неприемлемость биометрии в связи с её ассоциацией с криминалистикой (преступностью).

Заключение. В целом внедрение БМИТ в системы идентификации, которые используются в рамках областей применения, описанных выше, даёт возможность обеспечить безопасность как физических объектов, например, зданий, сооружений, так и информационную безопасность банковских программ, терминалов, порталов государственных и иных услуг, социальных, медицинских программ и т п.Системы или приложения, разработанные на основе БМИТ, входят в повседневный обиход людей также, как например, уже вошло использование мобильных телефонов. Авторы выражают надежду, что обеспечение безопасностина основе БМИТ и, прежде всего, социально-экономической безопасности, будет способствовать широкому использованию биометрии.

СПИСОК ЛИТЕРАТУРЫ

1. Маркелов К.С., Нечаев В.В. Систематизация и классификация методов биометрической идентификации. Современные информационные технологии в управлении и образовании: Сборник научных трудов. В 3-х ч. – М.: ФГУП НИИ «Восход», 2013. – Ч.1 – с. 100 - 109
2. Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника, 2002.

УДК 004.056.53

О ЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Марков Алексей Сергеевич, Фадин Андрей Анатольевич,
Цирлов Валентин Леонидович, Рауткин Юрий Владимирович,
ЗАО «НПО «Эшелон»,
Россия, Москва, ул. Электрозаводская, д. 24,
e-mails: am@cnpo.ru; mail@cnpo.ru; z@cnpo.ru; mail@npo-echelon.com

Аннотация: Показана роль SIEM-систем в структуре управления информационной безопасностью предприятия. Выделены основные компоненты SIEM-системы. Обоснованы показатели выбора SIEM-системы. Сделан обзор российского и международного рынка SIEM-решений. Типовая архитектура и принципы функционирования рассмотрены на примере программного комплекса «KOMRAD Enterprise

SIEM». Рассмотрены проблемные вопросы внедрения SIEM-систем. Представлен опыт разработки и внедрения отечественной SIEM.

Ключевые слова: *события информационной безопасности, мониторинг, управление безопасностью, анализ данных, правила корреляции.*

CENTRALIZING OF INFORMATION SECURITY CONTROL

Alexey S. Markov, Andrei A. Fadin,
Valentin L. Tsirlov, Yurii V. Rautkin,
NPO Echelon,
Russia, Moscow, Elektrozavodskaya ul, 24,
e-mails: am@cnpo.ru; mail@cnpo.ru; z@cnpo.ru; mail@npo-echelon.com

Abstract: The role of SIEM-systems in the management structure of the enterprise information security is shown. The basic components of SIEM-system are obtained. Based indicators for SIEM-selection system are substantiated. The review of the Russian and international market is done. Typical architecture and operating principles are considered by the example of KOMRAD Enterprise SIEM. The issues of implementing SIEM-systems are considered. The experience in the development and implementation of national SIEM is presented.

Keywords: *information security events, monitoring, SIEM, data analysis, correlation rules.*

Введение. 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 [1], [5]. 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. В 2005 году аналитическое агентство Gartner объединило термины Security Information Management (SIM) и Security Event Management (SEM). Так появилось понятие Security Information and Event Management (SIEM) – система, предназначенная для анализа информации, поступающей от различных систем [9].

SIEM можно определить как класс решений в области информационной безопасности, ориентированных на поддержку процессов управления как безопасностью, так и всей IT-инфраструктурой предприятия [2], [3], [4]. Решение SIEM позволяет проводить [6]:

- централизованный сбор и анализ данных журналов событий СЗИ, АРМ, серверов и сетевого оборудования;
- удаленный контроль параметров конфигурации и работы автоматизированных рабочих мест с помощью инсталлированного программного агента;
- оперативное оповещение и реагирование на внутренние и внешние угрозы безопасности автоматизированной системы;
- контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности АС в любые моменты времени.

Важнейшей особенностью SIEM-решений является возможность выявления неизвестных компьютерных атак, т.е. атак, не выявляемых сигнатурными методами [7].

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.

Сенсоры, как правило, располагаются в каждом сегменте (и даже узле сети). Центр управления и хранилище журналов событий чаще всего находятся в контролируемой зоне, рядом либо с АРМ администратора безопасности, либо с АРМ системного администратора АС.

Сенсоры должны поддерживать различные протоколы взаимодействия и иметь возможность настройки новых протоколов и входных форматов. 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» [8]. 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.

Заключение. 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.

СПИСОК ЛИТЕРАТУРЫ

1. Гарнаева М.А., Функ К. Kaspersky Security Bulletin 2013. Вопросы кибербезопасности. 2014. № 3 (4). С. 65-68.
2. Давидич В. Особенности внедрения и эксплуатации решения класса SIEM // Защита информации. Инсайд. 2011. № 5. С. 64-67.
3. Ефимов И.Э., Зюзько И.В. Построение эффективной системы управления и мониторинга информационной безопасности // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. 2014. № 2 (14). С. 62-66.
4. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. 2014. Т.3. № 1 С. 170-180.
5. Котенко И.В., Юсупов Р.М. Текущее состояние и тенденции развития в области построения безопасных компьютерных систем // В сборнике: 5-я Российская мультиконференция по проблемам управления материалы конференции «Информационные технологии в управлении» (ИТУ-2012). 2012. С. 671-675.
6. Марков А. С., Фадин А. А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4. С.80-81.
7. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.
8. Фадин А.А. На пути к развертыванию центра управления информационной безопасностью предприятия // Connect! Мир связи: наука. Бизнес. Управление. 2013. № 4. С.57-60.
9. Nicolett M., Kavanagh K.M. Critical Capabilities for Security Information and Event Management. Gartner Inc, 2014. 20 p.

УДК 621.391.28
ББК 32.811.

СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕРРИТОРИАЛЬНЫХ УЧРЕЖДЕНИЯХ БАНКА РОССИИ

Мошак Николай Николаевич,
НТЦ ПАО «Информационные телекоммуникационные технологии»,
Россия, Санкт-Петербург, ул. Кантемировская, д. 8,
e-mail: nnmoshak49@male.ru.

Аннотация: В статье приводится эволюция создания и применения систем мониторинга информационной безопасности в территориальных учреждениях Банка России

Ключевые слова: *информационная безопасность; система мониторинга информационной безопасности; Банк России*

INFORMATION SECURITY MONITORING SYSTEMS IN REGION OFFICIS OF BANK RUSSIA

Moshak Nikolai Nikolaevich,
NTC JSC «Information and telecommunication technologies»,
Russia, Saint-Petersburg, ul. Kantemirovskaya, d. 8,
e-mail: nnmoshak49@male.ru.

Abstract: Evolution of building and application security information monitoring systems in region offices of Bank Russia are proposed.

Keywords: *information security; security information monitoring system; Bank of Russia*

Работа Территориального учреждения Банка России в современных условиях характеризуется многообразием функциональных и управленческих задач, требующих постоянного совершенствования системы внутреннего контроля. При этом решение практически всех задач осуществляется с использованием распределенных автоматизированных банковских систем (АБС). Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения (СТО БР ИББС-1.0-2010)» [1] в качестве одного из направлений обеспечения информационной безопасности (ИБ) АБС определяет развитие механизмов внутреннего контроля и мониторинга ИБ.

Известно [2], что одной из ключевых проблем ИБ АБС является проблема инсайдеров или администраторов. Традиционные технические средства защиты от внешних угроз против инсайда не эффективны, поскольку инсайдер изначально, по своему статусу, легально допущен к информации. Вопрос в том, как он использует информацию — в соответствии с должностными обязанностями, учтенными в политике безопасности, или нет. Инсайд возникает во втором случае, но отличить одно от другого сложно. Поэтому и появляется необходимость четкого структурирования доступа пользователей к информационно-техническим ресурсам, контроля и анализа их деятельности по доступу к таким ресурсам и формирования вывода о направленности этих действий.

В этих условиях эффективный внутренний контроль за состоянием ИБ возможен только при своевременной и адекватной оценке значительных объемов информации. Анализ существующей практики показывает, что на уровне Территориального учреждения Банка России в сутки в рамках технологического мониторинга регистрируются миллионы различного рода событий, 99,9% из которых являются информацией о штатной работе системных и прикладных процессов, проведении регламентных работ. При этом события информационной безопасности к общему количеству первичных событий составляют лишь сотые доли процента и в основном связаны с регламентными модификациями программного обеспечения.

Главная проблема процесса мониторинга и анализа событий ИБ при ручной обработке – это невозможность обнаружения деструктивных воздействий на АБС и их элементы в реальном времени при визуальном контроле записей в их штатных журналах аудита. Таким образом, выявление реальной угрозы, например, вирусного заражения, комбинированной атаки, с целью несанкционированного доступа к информационным активам, и оперативное принятие управленческого решения возможно только с использованием автоматизированных технологий контроля и, прежде всего, автоматизированного мониторинга ИБ.

Основной задачей мониторинга ИБ является контроль и определение соответствия поведения легальных пользователей АБС правилам ее политики информационной безопасности, выявление в реальном времени фактов как неправомерных или ошибочных действий пользователей и администраторов, так и реализуемых возможными нарушителями атак на информационные ресурсы АБС, а также выдачи рекомендаций администрации АБС для необходимой реакции на технологический процесс, а также прогнозирование состояния ИБ АБС, на основании которого АБС обретает возможность выявления и упреждения угроз на ранней стадии их возникновения.

Мониторинг ИБ является одной из важнейших составляющих ее политики информационной безопасности и составной частью модели непрерывного циклического процесса менеджмента ИБ организации (так называемой, модели Деминга), которая является основой международных стандартов менеджмента информационной безопасности (ISO/IEC IS 27001), менеджмента качества (ГОСТ Р ИСО 9001) и других стандартов.

Активное участие в решении задачи создания указанных систем принимал Опорный объект по тиражированию интегральных систем мониторинга информационной безопасности, созданный на базе Главного управления Банка России по Ленинградской области в 2002 году. В течение десяти лет было создано ряд систем мониторинга ИБ и их модификаций для платежных и информационных (неплатежных) АБС.

Изначально автоматизация мониторинга ИБ была проведена для объектов учетно-операционной системы платежных АБС (система «Ромб-ЛО-М»). На данном этапе развития систем мониторинга ИБ была решена задача автоматизации сбора и анализа первичных событий мониторинга с возможностью оперативного предоставления информации о событиях ИБ в целом на

всем комплексе технических средств, задействованных в обеспечении работоспособности платежных АБС. Опорным объектом с 2008 года осуществлялось сопровождение внедрения и эксплуатации системы «Ромб-ЛО-М» для платежного сегмента в 36 ТУ Банка России.

На следующем этапе была разработана аналогичная по своим функциональным характеристикам система «Блокада-Инфо», обеспечивающая контроль состояния ИБ для двадцати одной неплатежной АБС.

Однако данные системы мониторинга обеспечивали анализ данных от множества подконтрольных объектов, лишь в рамках того сегмента локальной вычислительной сети, в котором они функционировали. При этом не учитывалась возможная взаимосвязь сигналов тревоги от разных источников, а причинно-следственные связи их возникновения все равно приходилось устанавливать вручную, дополняя результаты анализа организационными расследованиями. Кроме того, в правилах анализа (сигнатурах) не предусматривалась временная корреляция наступления событий ИБ, т. е. отсутствовала возможность прогнозирования их наступления. Результаты расследований инцидентов ИБ (реализованных угроз ИБ) и аналитические справки, предоставляемые на плановой основе, также формировались непосредственно экспертами вручную. Таким образом, задача автоматизации внутреннего контроля была решена не полностью.

Для решения указанных проблем в 2011 году была создана система «Монитор-регион/Инцидент», позволяющая проводить анализ коррелированных событий ИБ (КСИБ) от разных типов подконтрольных объектов, функционирующих в различных сегментах сети и производить автоматизированную обработку инцидентов ИБ, связанных с реализацией угроз.

С целью унификации процессов контроля ИБ в 2013 году системы «Ромб-ЛО-М», «Блокада-Инфо» и «Монитор-регион\Инцидент» были объединены в функционально завершенный комплекс «Единая система мониторинга информационной безопасности Главного управления Банка России по Ленинградской области» (ЕСМИБ-ТУ-ЛО) на базе единой системно-технической платформы.

Целями создания ЕСМИБ-ТУ-ЛО являются:

– повышение эффективности управленческой деятельности и внутреннего контроля ТУ Банка России;

– автоматизированный контроль выполнения требований нормативных документов Банка России по ИБ в реальном времени;

– обеспечение устойчивого функционирования информационно-телекоммуникационной системы ТУ Банка России;

– повышение качества и эффективности мониторинга ИБ ТУ Банка России.

Объектами мониторинга ЕСМИБ ТУ-ЛО является совокупность платежных и информационных АБС, средств защиты информации и антивирусного контроля, а также сетевого оборудования

ЕСМИБ-ТУ-ЛО имеет трехуровневую архитектуру (Рисунок 1). Задачей первого уровня мониторинга является сбор и представление в унифицированном внутреннем формате информации о событиях мониторинга. Источниками событий мониторинга являются как собственные средства системы, так и средства регистрации событий, функционирующие в составе контролируемых типовых автоматизированных систем Банка России, и хранящие события в своих журналах (автоматизированных рабочих мест, штатных журналов аудита операционных систем, систем управления базами данных, маршрутизаторов, систем защиты и антивирусного контроля и др.).

Состав источников событий мониторинга определен Банком России исходя из потребности контроля действий пользователей и мониторинга ИБ для автоматизированных систем уровня ТУ.

Главный компонент первого уровня – подсистема сбора. Результатом работы первого уровня мониторинга является набор событий мониторинга в унифицированном формате представления, не зависящем от типа источника, которые формируют собственные программные агенты.

Задачей второго уровня является анализ первичных данных мониторинга и формирование сообщений о событиях ИБ, их сохранение в базе данных, оперативное информирование персонала о зафиксированных событиях, обеспечение проведения расследования, т. е. поддержка запросов к базе данных, позволяющих установить контекст события ИБ: место, время, имя пользователя и прочее, а также сопутствующие события.

Третий уровень ЕСМИБ-ТУ-ЛО представлен подсистемами идентификации КСИБ и обработки коррелированных событий ИБ (КСИБ).

На третьем уровне в подсистеме идентификации осуществляется совместный анализ сообщений о событиях ИБ (по субъектам, объектам и критичным ресурсам АБС уровня ТУ) от разнотипных источников и формирование КСИБ. формирование (идентификация) КСИБ осуществляется в результате взаимоувязанного анализа событий ИБ от разнотипных объектов в соответствии с набором правил анализа, сформированных с учетом требований конкретных положений нормативных документов Банка России по ИБ. Идентификация может выполняться как по мере поступления входных данных в режиме, максимально приближенном к режиму реального времени, так и в отложенном режиме, по запросам персонала. При этом каждое идентифицированное КСИБ содержит ссылку на нарушение конкретных требований нормативных документов Банка России по ИБ и передается в подсистему обработки.

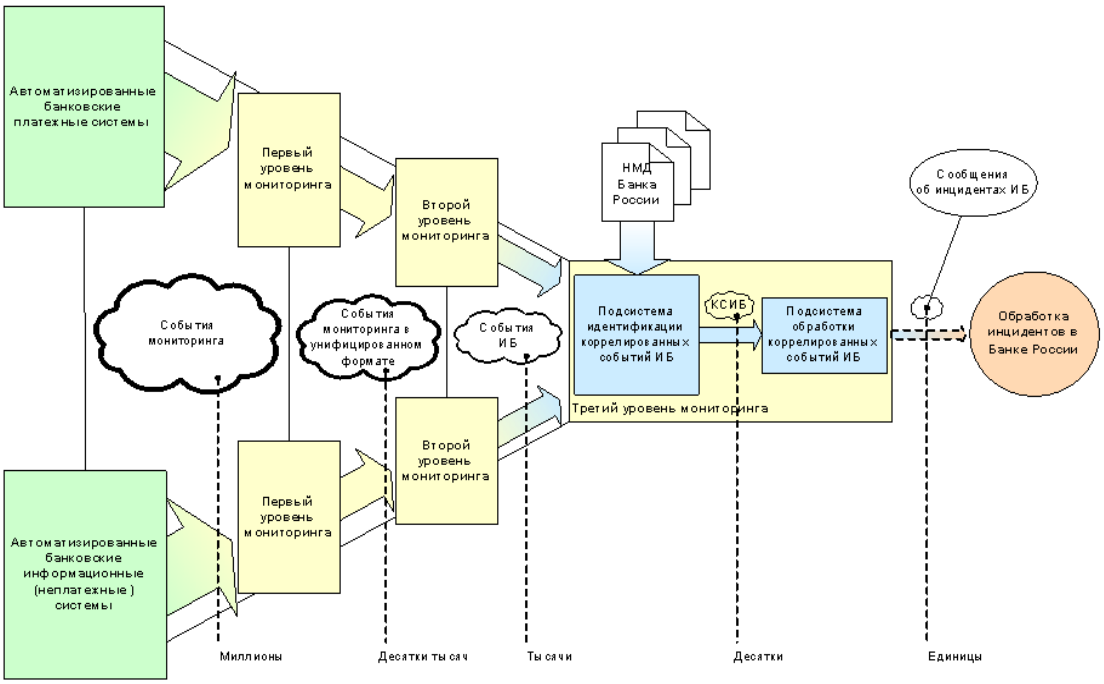


Рис. 1. Обобщенная архитектура ЕСМИБ-ТУ-ЛО

В оперативном режиме выполняется анализ событий ИБ из нескольких источников одновременно без переписывания данных в промежуточное хранилище, с сохранением специфики и уникальности информации об источниках данных. Анализ событий ИБ проводится как независимо для каждого объекта мониторинга, так и с учетом взаимных связей (корреляций) событий ИБ, зафиксированных для нескольких объектов мониторинга в составе систем уровня ТУ.

В рамках постановки задач Опорным объектом были сформулированы принципы анализа признаков, идентифицирующих угрозы ИБ, а также принципы анализа КСИБ. Формализация этих признаков, реализованных в настройках системы, определяется как правила анализа. В настоящее время в системе задействовано около ста правил анализа КСИБ. Для упрощения создания правил анализа в единой системе имеются специальные визуальные средства. Процесс описания правил осуществляется декларативным способом в специальном редакторе без элементов программирования.

Подсистема обработки КСИБ обеспечивает этапность обработки в соответствии с назначенными ролями персонала (Регистратор, Ответственный, Руководитель и др.). В зависимости от назначенной роли, персоналу доступны различные функции по обработке КСИБ. Например, разрешение (закрытие) коррелированного события ИБ может выполнить только пользователь с ролью «Ответственный» и т. д.

Использование Web-технологий позволяет подключать новых ответственных лиц без установки дополнительного программного обеспечения на их рабочие места. Доступ осуществляется по http-протоколу из Интернет-браузера, что предоставляет возможность работы с системой, не привязываясь к определенному рабочему месту. Обработка КСИБ осуществляется в соответствии с регламентом реагирования на инциденты ИБ, т.е. с учетом режимов обработки, реализации функций пользователей и содержания заполняемых форм.

Сообщения о сформированном коррелированном событии безопасности отображаются на АРМ эксперта-аналитика (работника службы безопасности) и направляются ему по электронной почте. Дальнейший анализ и уточнение обстоятельств возникновения инцидента ИБ осуществляется при участии Руководителя группы обработки инцидентов ИБ.

При обработке инцидентов реализована возможность оценки влияния обнаруженного инцидента безопасности на технологические процессы ТУ: а именно, указания типов

информационных активов, степени тяжести последствий, конкретизации угрозы информационной безопасности, определения воздействия на средства защиты информации. Система предоставляет возможность гибкой настройки последовательности обработки КСИБ.

Эффект применения ЕСМИБ-ТУ-ЛО можно наглядно представить на примере формирования следующих коррелированных событий ИБ:

1. Обнаружение вредоносного кода на съемном машинном носителе.
2. Регистрация и работа в платежной АБС от имени пользователя, находящегося в отпуске.

При обнаружении вредоносного кода коррелированное событие формируется на основе событий безопасности, полученных из двух источников: системы защиты от воздействий вредоносного кода (например, Антивирус Касперского) и системы контроля использования устройств ввода-вывода информации и коммуникационных портов (например, системой «Контроль-ПУ»).

Это позволяет в режиме реального времени не только обнаружить факт заражения вредоносным кодом, но и установить конкретный источник, что значительно ускоряет процесс расследования, локализации и предотвращения дельнейшего заражения информационно-телекоммуникационной системы ТУ Банка России.

Во втором примере сообщение формируется на основе событий безопасности от следующих источников: автоматизированной системы «Внутрихозяйственная деятельность» (предоставляет информацию о периоде отпуска пользователя), операционной системы Windows или платежной АБС (предоставляют информацию о регистрации в системе от имени учетной записи пользователя).

Таким образом, если в период отпуска сотрудник регистрируется в какой-либо из систем (идентификатор определяется по карточке сотрудника в базе ЕСМИБ-ТУ-ЛО), формируется КСИБ.

По результатам обработки КСИБ система обеспечивает построение настраиваемых отчетных форм, которые могут быть использованы при создании документационного обеспечения деятельности службы безопасности.

Отчеты по результатам обработки КСИБ включают несколько форм и позволяют получать информацию:

– о количестве КСИБ, находящихся в обработке;
– общее количество нарушений требований ИБ.

ЕСМИБ-ТУ-ЛО предусматривает необходимые интерфейсы (Электронная почта, WEB-интерфейс, доступ к базе данных инцидентов ИБ) для передачи данных о КСИБ в Банк России на централизованный уровень обработки инцидентов ИБ и отчетов.

В 2013 году Банком России в рамках реализации Концепции построения системы обеспечения информационной безопасности Территориального учреждения была поставлена задача по разработке типового проектного решения единой системы мониторинга информационной безопасности Территориального учреждения (ЕСМИБ ТУ) на базе ЕСМИБ-ТУ-ЛО по результатам ее эксплуатации.

Типовое проектное решение ЕСМИБ ТУ будет протиражировано в 2014 году во все ТУ Банка России. В основу типового проектного решения ЕСМИБ ТУ положены принципы, апробированные в процессе десятилетней эксплуатации вышеуказанных систем мониторинга ИБ

– расширяемость перечня входных данных;
– возможность распределенной обработки входных данных;
– адаптируемость к территориально распределенным АБС;
– масштабируемость системы;
– доступ персонала к системе на основе ролей (администратор, АИБ, пользователи и др.);
– Web-технологии;
– расширяемость перечня способов оповещения персонала.

Эффективность применения таких подходов подтверждена также опытом внедрения и тиражирования в ТУ Банка России систем мониторинга ИБ, служащих основой создаваемой ЕСМИБ ТУ.

Внедрение ЕСМИБ ТУ позволит значительно сократить эксплуатационные расходы на системы указанного класса в целом по Банку России, улучшит качество объективной информации по результатам обработки инцидентов ИБ, оперативность принятия управленческих решений в условиях возникновения нештатных ситуаций, что в целом повысит эффективность внутреннего контроля по данному направлению деятельности ТУ и обеспечит устойчивое и безопасное функционирование ее информационно-телекоммуникационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
2. Валерий Васильев. Стандартизация безопасности финансовой системы — гибкая, но обязательная (Интервью А.П. Курило). PC Week/RE, №06/2007.

СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И РИСКА НА ОСНОВЕ АЛЬТМАНОВСКОГО ПОДХОДА

Пичугин Юрий Александрович[1], Кондрашков Анатолий Викторович[2],
[1] Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, Санкт-Петербург, ул. Большая Морская, д. 67,
[2] Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, улица Садовая, д. 21,
e-mails: yury-pichugine@mail.ru, ankon69@mail.ru.

Аннотация: Рассмотрен метод Альтмана оценки экономической безопасности и риска. Оценка конкретного предприятия рассматривается в терминах проверки статистических гипотез. Приводятся критерии относительной вариабельности и относительной стабильности. Рассмотрены вычислительные аспекты.

Ключевые слова: *вектор Альтмана; эллипсоиды риска и надежности; проверка гипотез; относительная вариабельность и стабильность*

THE STATISTICAL ESTIMATION OF ECONOMIC STABILITY AND RISK ON THE BASIS OF ALTMAN'S METHOD

Pichugin Yu. A. [1], Kondrashkov A.V. [2],
[1] Saint-Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, St. Petersburg, ul. Bolshaya Morskaya. 67,
[2] Saint-Petersburg State University of Economics and Finance,
Russia, St. Petersburg, Sadovaya, d. 21,
e-mails: yury-pichugine@mail.ru, ankon69@mail.ru.

Abstract: Altman's method of the economic stability and risk estimating is reviewed. An estimation of specific enterprise is considered in terms of the statistical hypotheses testing. Criteria of relative variability and relative stability are given. Computational aspects are considered too.

Keywords: *Altman's vector; ellipsoids of risk and trust; hypotheses testing; relative variability and stability*

Введение

Понятие экономической безопасности в самом общем смысле включает в себя два взаимно дополняющих момента – это внешняя безопасность, определяемая состоянием внешней экономической среды и взаимодействием с ней, включая экономических партнеров, конкурентов и прочее, а также внутренняя безопасность, в которой основным фактором, несомненно, является состояние предприятия и его стабильность. Для оценки состояния предприятия необходимы, как минимум, две вещи – это критерии оценки состояния и данные, по которым эти оценки производятся. Ниже рассматривается один из видов оценки состояния предприятия и вычислительные аспекты, связанные с реализацией этой оценки по имеющимся данным.

1. Оценка экономической безопасности предприятий по методу Э. Альтмана

Известный экономист Эдвард Альтман предложил следующий метод оценки состояния предприятия. Для пяти экономических показателей x1,x2,,…,x5 строится линейная форма [1,2]

$$\varphi(X)=C^{т}X,$$

$$X^{т}=(x1,x2,,\ldots,x5),\quad C^{т}=(c1,c2,\ldots,c5).$$

(т– знак транспонирования).

Коэффициенты этой линейной формы образуют пятимерный вектор Альтмана C, все компоненты которого определяются по статистическим данным. Принцип вычисления состоит в нахождении по методу наименьших квадратов в пространстве выбранных экономических показателей гиперплоскости, которая с минимальной квадратичной ошибкой воспроизводит статистику этих показателей для группы наиболее успешных и стабильных предприятий, акции которых котируются на развитых рынках. Таким образом, вектор Альтмана суть нормаль к гиперплоскости наилучшим образом воспроизводящей статистику стабильных предприятий. Приведем список этих экономических показателей согласно Э. Альтману:

x1 – отношение оборотного капитала/сумме активов;

x2 – отношение нераспределенной прибыли/сумме активов;

x3 – отношение операционной прибыли/сумме активов;

x4 – отношение рыночной стоимости акций/задолженности (для компаний, акции которых котируются на бирже) или отношение балансовой стоимости собственного капитала/привлеченному капиталу (для компаний, акции которых не котируются на бирже);

x5 – отношение прибыли/сумме активов.

Два значения φC и φR ($\varphi C>\varphi R$) задают разбиение области G допустимых значений X на три подобласти:

$GC=\{X: X\in G, \varphi(X)>\varphi C\}$ – экономической безопасности,

$GR=\{X: X\in G, \varphi(X)<\varphi R\}$ – несостоятельности (риска) и

$GN=\{X: X\in G, \varphi R \le\varphi(X)\le\varphi C\}$ – неопределенности.

Например, по данным Альтмана

$\varphi(X)=1{,}2x1+1{,}4x2+3{,}3x3+0{,}6x4+0{,}999x5$

для компаний на развитых рынках, акции которых котируются на бирже. При этом значения, определяющие границы зон безопасности и риска, соответственно равны φR =1,8 и φC=3.

Сущность альтмановского подхода состоит в сравнении показателей отдельного предприятия (X) с общим экономическим фоном.

2. Основные предположения относительно вероятностного распределения и вычисление вектора Альтмана

Предположим, что вектор экономических показателей X подчиняется многомерному нормальному распределению. Такое предположение допустимо, когда поле рассеяния имеющихся данных, а, соответственно, и вероятностное распределение X достаточно локализовано в центральной части области допустимых значений G.

Пусть имеется выборка данных по стабильным предприятиям {Xj, j=1,2,..n} за достаточно большой период наблюдений. Вычислим оценки вектора средних значений

$$\Theta C =n-1\Sigma j=1,..,n(Xj) \qquad (1)$$

($\Sigma j=1,..,n$ – знак суммирования) и матрицы взаимных ковариаций

$$VC = (n-1)-1\Sigma j=1,..n(Xj-\Theta C)(Xj-\Theta C)т. \qquad (2)$$

Пусть вычислена ортогональная матрица P, такая, что

$$PтVCP=D=diag(d1,d2,\ldots,d5).$$

Столбцы матрицы P можно расположить в таком порядке, чтобы выполнялось условие $d1\ge d2\ge\ldots\ge d5$. Тогда нормированный вектор Альтмана C=P5, где P5 – последний столбец матрицы P, соответствующий наименьшему собственному значению (d5). Действительно, сумма квадратов отклонений всех значений Xj от гиперплоскости $CтX=\varphi 0$ ($\varphi 0=CтΘC$), равна минимальному значению (n–1)d5. Величину φC можно определить исходя из выбранного уровня доверия (1–α), как границу левосторонней критической области для величины (d5)–1/2Cт(X–ΘC) т.е.

$$\varphi C=CтΘC – (d5)1/2t\alpha/2n-1 \qquad (3)$$

($t\alpha/2n-1$ – квантиль распределения Стьюдента). Это означает, что для стабильных предприятий вероятность оказаться ниже уровня φC равна $\alpha/2$, так как критерий Стьюдента является двусторонним. При наличии выборки данных по неэффективным предприятиям, в принципе, может быть вычислен другой вектор Альтмана, при этом вполне может оказаться, что оценки этих векторов не совпадают. Для того, чтобы не усложнять модель, значение φR можно вычислять, используя вектор C, полученный по данным стабильных предприятий, заменяя в формуле (3) ΘC на вектор средних значений по несостоятельным предприятиям ΘR, а значение d5 на CтVRC, т.е.

$$\varphi R =CтΘR +(CтVRC)1/2t\alpha/2k-1,$$

где VR – матрица взаимных ковариаций X, оцененная по выборке объема k данных несостоятельных предприятий. Здесь знак «+» означает, что φR является границей правосторонней критической области. В этом случае при вычислении φR необязательно брать значение α такое же, как и при вычислении φC, но соображения надежности требуют, чтобы оно было не больше, чем в первом случае. Кроме того, желательно, чтобы при вполне приемлемых значениях α не нарушалось условие $\varphi C>\varphi R$, тогда полученные значения φC и φR можно будет считать вполне объективными. Однако большой выборки данных по несостоятельным предприятиям может не оказаться из-за короткого времени их существования или пребывания в критическом состоянии. Тогда значение φR вычисляется по формуле (3), как граница левосторонней критической области при предельно допустимом значении α, но существенно меньшем, чем при вычислении φC.

Предположим, что для конкретного, оцениваемого по Альтману, предприятия имеются наблюдения {Xt, t=1,2,…,T}за некоторый период, T – продолжительность наблюдаемого периода. Это позволяет нам, используя формулы (1) и (2), получить аналогичные оценки параметров Θ и V, предполагая, что вектор экономических показателей X оцениваемого предприятия подчиняется многомерному нормальному распределению $X\sim N(\Theta,V)$.

3. Задача Лагранжа

При фиксированном значении f0 функция f(X) плотности распределения вероятностей вектора X задает в 5-мерном пространстве гиперповерхность уровня, которая хорошо известна как эллипсоид рассеяния f(X)=f0.

Для начала выясним, при каком значении fR этот эллипсоид WR={X: f(X)=fR}, который назовем эллипсоидом риска, соприкасается с критической границей, заданной равенством $\varphi(X)=\varphi R$, а заодно и вычислим точку прикосновения XR. Решение этой задачи строится из геометрического соотношения

$$\text{grad } f(X)=\gamma\cdot\text{grad } \varphi(X) \quad (\gamma \text{ - скаляр}),$$

означающего, что в точке касания вектор нормали к эллипсоиду риска и вектор нормали к гиперплоскости $\varphi(X)=\varphi R$ (вектор Альтмана) коллинеарны.

Функция плотности распределения f(X)=f(X,Θ,V) задается формулой [3]

$$f(X) = (2\pi)-5/2(\det V) -1/2\cdot\exp(-0,5\cdot(X-\Theta)\text{т } V-1(X-\Theta)) \quad (4)$$

В этом случае функцию Лагранжа удобно записать в виде

$$L(X,\lambda)=\ln f(X) - \lambda(\varphi(X) - \varphi R). \quad (5)$$

Дифференцируя выражение (5) по компонентам X и λ приравниваем частные производные к нулю. Полученные соотношения можно записать в матричной форме

$$V-1(XR - \Theta)=\lambda C, \quad C\text{т}XR =\varphi R, \quad (6)$$

Нетрудно видеть, что решение задачи, сформулированное условиями (6), дается относительно простыми формулами [4,5]

$$\lambda=(\varphi R - C\text{т}\Theta)(C\text{т}VC)-1, \quad XR = \Theta + \lambda VC \quad (7)$$

4. Проверка статистических гипотез

С учетом выше изложенного статистическая проверка безопасности (степени риска) сводится к проверке гипотезы

$$HR : X\in GR. \quad (8)$$

Это означает проверку предположения, что состояние экономических показателей данного предприятия может (пусть и случайно) оказаться в зоне банкротства.

В одномерном случае при нормальном распределении, проверяя статистическую гипотезу, мы имеем в качестве границы критической области две точки, расположенные симметрично относительно центра предполагаемого распределения. В нашем 5-мерном случае, если проверяется гипотеза

$$H0:X= X*$$

границей критической области будет эллипсоид Wα с центром в точке X∗, такой, что функция плотности указанного выше распределения принимает на нем постоянное значение, а вероятность того, что точка X с координатами {x1,x2,,…,x5} принадлежит области, ограниченной этим эллипсоидом, равна 1− α (здесь α − уровень значимости). Т. е. это один из эллипсоидов рассеяния (см. выше). В нашем случае, когда гипотеза HR имеет вид (8), эту гипотезу можно рассматривать как совокупность простых гипотез H0:X=X∗, где X∗∈GR. Тогда общей границей пересечения всех критических областей будет плоскость, лежащая в области допустимых значений G. Эта плоскость будет являться огибающей поверхностью семейства эллипсоидов Wα при условии, что центры эллипсоидов (параметры сдвига семейства распределений Θ) пробегают границу области GR. Проверку такой гипотезы можно осуществить по следующему алгоритму, основанному на том, что аргумент и параметр сдвига в функции плотности распределения занимают симметричное положение.

Вычислим вероятностную меру области, ограниченной эллипсоидом риска

$$WR=\{X: f(X)=fR\}, \quad fR=f(XR).$$

Тогда гипотеза HR отвергается на уровне значимости α, если вероятностная мера области, ограниченной эллипсоидом риска больше выбранного уровня доверия (1−α), это в точности и означает, что полученная оценка параметра Θ лежит за пределами критической области проверяемой гипотезы.

Если задаться вопросом оценки надежной (устойчивой) работы предприятия, то следует проверять гипотезу

$$HN:X\in GN\cup GR.$$

В этом случае необходимо найти точку касания XC эллипсоида рассеяния с гиперплоскостью $\varphi(X)=\varphi C$. Решение этой задачи также дается формулами (7) при замене значений φR и XR на φC и XC, соответственно. Точка XC определяет, в свою очередь, эллипсоид надежности (см. рис. 1).

$$WC=\{X: f(X)=fC\}, \quad fC=f(XC).$$

Вероятностная мера области, ограниченной эллипсоидом надежности, также сравнивается с выбранным доверительным уровнем (1−α). При этом, если эта вероятностная мера превышает значение (1−α), состояние предприятия может быть оценено, как вполне надежное по Альтману.

5. Вырожденность распределения и относительно малый размер выборки

Вполне вероятно, что оценка матрицы V может оказаться вырожденной (например, при небольшом объеме выборки), а, соответственно, и распределение вектора X будет вырождено. В этом случае необходимо найти ортогональную матрицу Q такую, что

$$Q\text{т}VQ =\Lambda=\text{diag}(\lambda1,\lambda2,\ldots,\lambda5),$$

где столбцы матрицы Q расположены так, что $\lambda 1 \geq \lambda 2 \geq \ldots \geq \lambda 5$. Вырожденность матрицы V равносильна тому, что, по крайней мере, $\lambda 5=0$. В этом случае в формуле (4) вместо $(2\pi)-5/2(\det V)-1/2$ будет стоять $(2\pi)-m/2(\det \Lambda m)-1/2$, а вместо $V-1$ будет стоять матрица $Qm(\Lambda m)-1Qmт$. Здесь Λm - матрица порядка m ($1 \leq m \leq 5$, равенство справа соответствует невырожденному случаю). Λm на главной диагонали содержит только ненулевые значения матрицы Λ, а Qm содержит только столбцы Q, отвечающие этим ненулевым значениям. Формулы (7), как нетрудно видеть, останутся прежними, т.к. $Qm\Lambda mQmт=V$, а величина $CтVC$ может обращаться в ноль только в случае, когда вектор Альтмана ортогонален направлениям всех ненулевых главных компонент (случай полной относительной стабильности, см. ниже), т. е. эллипсоиды WR и WC не существуют.

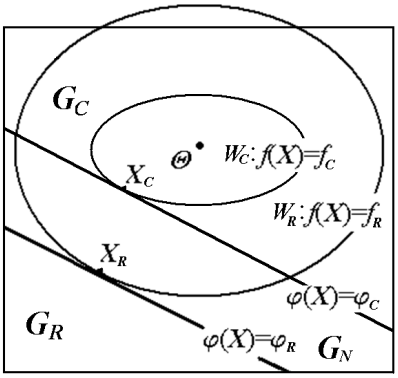


Рис. 1. Эллипсоиды риска и надежности

Вырожденность распределения, в свою очередь, приводит к тому, что вероятностные меры эллипсоидов рассеяния (риска и надежности) придется вычислять в пространстве вектора меньшей размерности. Это ни в коей мере не усложнит задачу, а возможно и наоборот, несколько упростит ее.

В случае относительно небольшого размера выборки (как, впрочем, и в случае большого размера) для проверки гипотезы $HR:X \in GR$ можно воспользоваться статистикой, которая при верной гипотезе HR (фактически мы проверяем $H'R:X=XR$) имеет распределение достаточно близкое к хи-квадрат с m степенями свободы, т.е.

$$r = (XR-\Theta)тQm(\Lambda m)-1Qmт(XR-\Theta) \sim \chi 2m. \quad (9)$$

Кроме того, компоненты вектора

$$S=(\Lambda m)-1/2Qmт\,(XR-\Theta) \quad (10)$$

будут независимы и, в тех же предположениях, будут иметь распределение Стьюдента с числом степеней свободы $\nu=T-1$. Таким образом, если $r > \chi 2m(\alpha)$ (односторонний критерий) или для какого-либо значения $i \in \{1,2,\ldots m\}$ $|si| > t\alpha/2\nu$ (двусторонний критерий), HR отвергается. Проверка гипотезы $HN:X \in GN \cup GR$ осуществляется аналогично. При этом в (9) и (10) используется значение XC. Независимо от выбора критерия вычисление точек касания RR и XC является необходимым условием, так как указанные распределения строятся на основе нормального распределения, а геометрические свойства последнего в этой ситуации играют ключевую роль. Именно эти свойства позволяют сводить проверку гипотез $HR:X \in GR$ и $HN:X \in GN \cup GR$ к проверке гипотез $H'R:X=XR$ и $H'N:X= XC$.

6. Относительная вариабельность и относительная стабильность

Вектор $Qт(X-\Theta)$ известен как вектор главных компонент исходного вектора X. Условие $\lambda 1 \geq \lambda 2 \geq \lambda 3 \geq \lambda 4 \geq \lambda 5$ располагает эти главные компоненты в порядке убывания дисперсии. Вычисление главных компонент будет весьма полезным в любом случае, так как дает дополнительную информацию о состоянии предприятия за период оценивания. В целях анализа введем следующие безразмерные показатели для случая ненормированного вектора Альтмана, которые при желании можно выразить в процентах: показатель относительной вариабельности

$$VA=\{CтVC(CтC)-1\}/trV$$

(tr – след матрицы) и показатель относительной стабильности

$$SA=1-\{CтVC(CтC)-1\}/\lambda 1.$$

Показатель относительной вариабельности (VA) дает отношение дисперсии в направлении вектора Альтмана (в опасном направлении) к общей дисперсии. Показатель относительной стабильности (SA) приближается к единице, когда дисперсия в направлении вектора Альтмана мала по сравнению с дисперсией первой главной компоненты, и приближается к нулю в противоположном случае. Последнее ($SA \approx 0$) может иметь двоякую природу. Такая ситуация имеет место, когда направление первой главной компоненты (максимальной дисперсии) близко к направлению вектора Альтмана, что, очевидно, нельзя характеризовать как относительно стабильное состояние. С другой стороны, эта ситуация ($SA \approx 0$) может возникнуть, когда все собственные значения V мало различимы

между собой, что бывает только при невырожденном распределении мало различимом по направлениям, т. е., в принципе, хаотичном.

7. Вероятностная мера области, ограниченной эллипсоидом рассеяния

Область произвольно взятого эллипсоида рассеяния с учетом (4) допускает представление в виде

$$\Omega=\{X\in R5:\ h(X-\Theta)\le\mu\},$$

где выражение

$$h(X-\Theta):=0{,}5\cdot(X-\Theta)^{T}V^{-1}(X-\Theta)$$

выделено из показателя степени в плотности f(X), а μ – значение уровня. Вероятностная мера области такого эллипсоида выражается формулами:

$$P(\Omega)=\int_{\Omega}f(\mathbf{X})\,d\mathbf{X}=c\int_{\Omega}\exp\big(-h(\mathbf{X}-\boldsymbol{\Theta})\big)\,d\mathbf{X}=\frac{\int_{\Omega}\exp\big(-h(\mathbf{X}-\boldsymbol{\Theta})\big)\,d\mathbf{X}}{\int\exp\big(-h(\mathbf{X}-\boldsymbol{\Theta})\big)\,d\mathbf{X}},$$

с учетом условия нормировки

$$c\int\exp\big(-h(\mathbf{X}-\boldsymbol{\Theta})\big)\,d\mathbf{X}=1.$$

После несложных преобразований формула вероятности приобретает вид:

$$P(\Omega)=\frac{1}{\Gamma(5/2)}\int_{0}^{\sqrt{\mu}}s^{4}e^{-s^{2}}\,ds.$$

Применяя интегрирование по частям, окончательно находим:

$$P(\Omega)=\operatorname{erf}\big(\sqrt{\mu}\big)-\frac{2\sqrt{\mu}(3+2\mu)\exp(-\mu)}{3\sqrt{\pi}},$$

где erf – стандартная функция ошибок. В итоговых расчетах следует брать $\mu=h(X*-\Theta)$, где $X*$ – точка касания.

После подстановки критических значений $\mu C=h(XC-\Theta)$ и $\mu R=h(XR-\Theta)$ в установленную выше формулу будут найдены требуемые вероятностные объемы $P(\Omega C)$ и $P(\Omega R)$ областей ΩC и ΩR, ограниченных эллипсоидами надежности (WC) и риска (WR), соответственно.

8. Связь с нелинейной оптимизацией

Рассмотренная выше задача Лагранжа о нахождении точки касания эллипсоида рассеяния с границей области устойчивости может быть сведена к задаче нелинейного программирования (ЗНП):

$$h(X-\Theta)\to\min,\ X\notin G*,$$

где область $G*$ допустимых значений вектора X определяется в зависимости от того, какой из эллипсоидов риска или надежности (см. выше) требуется найти. Фактически область G_* определяется одним неравенством $\varphi(X)\ge\varphi_*$, где следует принять одно из двух: либо $\varphi_*=\varphi_R$; либо $\varphi_*=\varphi_C$. Равноценная формулировка данной ЗНП: Требуется найти решение

$$\mathbf{X}_*=\operatorname{Arg}\min_{\mathbf{X}\in G_*}h(\mathbf{X}-\boldsymbol{\Theta})$$

Фактически это открывает путь к использованию программных продуктов, содержащих средства нелинейной оптимизации. В частности, сюда относится программа Microsoft Excel, обладающая надстройкой «Поиск решения». Другие возможности предоставляют системы компьютерной математики: Wolfram Mathematica, MathCAD, и т. д.

Заключение. Из приведенного выше следует вывод, что рассмотренная методика может иметь широкое применение в оценке риска и надежности различных предприятий. Все этапы этой методики принципиально осуществимы, что, в свою очередь, позволяет рассматривать ее в качестве основы при разработке программных продуктов для решения практических задач экономического мониторинга.

Авторы выражают глубокую признательность Заслуженному деятелю науки РФ, доктору технических наук, профессору Трофимову В.В. за весьма конструктивное обсуждение настоящей работы.

СПИСОК ЛИТЕРАТУРЫ

1. Altman Edward Managing Credit Risk, 2nd Edition. – John Wiley and Sons, 2008.
2. Altman Edward Corporate Financial Distress and Bankruptcy, 3rd edition. – John Wiley and Sons, 2005.
3. Себер Дж. Линейный регрессионный анализ. – М.: Мир,1980. – 456 с.
4. Пичугин Ю.А. Вероятностные оценки риска и надежности в экономике//Научная сессия ГУАП: Сб. докл.: В 3 ч. Ч1. Технические науки/СПб.: ГУАП, СПб., 2013. С. 195-196.
5. Пичугин Ю.А., Малафеев О.А. Об оценке риска банкротства фирмы // VI Междунар. конф. "Динамические системы: устойчивость, управление, оптимизация" (DSSCO'13), посвященная 95-летию со дня рождения Е.А. Барбашина, 1–5 октября 2013 года, г. Минск. С. 204-206.

УДК 51-74

МНОГОКРИТЕРИАЛЬНЫЙ ОПТИМИЗАЦИОННЫЙ ВЫБОР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЙ

Попова Елена Владимировна,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mail: Serana5@inbox.ru.

Аннотация: Рассмотрена задача многокритериального выбора вариантов построения системы защиты информации на предприятии. Предложена модификация методарандомизированных сводных показателей для исследования сложных объектов при недостатке информации весовых коэффициентов, заключающаяся в получении теоретического значения коэффициента изменения конкурентоспособности, на основе которого происходит рейтингование исследуемых систем. Представленырезультаты использованияметода на предприятии.

Ключевые слова: *система защиты информации; информационная безопасность предприятия; многокритериальный выбор; конкурентоспособность; экспертная оценка.*

MULTICRITERION OPTIMIZATION CHOICE OF INFORMATION SECURITY SYSTEMS FOR COMPANIES

Popova Elena,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str., 21,
e-mail: Serana5@inbox.ru.

Abstract: The problem of multi-choice options for building information security system in the company. A modification of the method of summary measures for randomized study of complex objects with a lack of information weights is to obtain the theoretical values of the coefficient changes competitiveness on which occurs ratings of the systems studied. The results of its use in the company.

Keywords: *system information security; information security company; multicriteria selection; competitiveness; expert evaluation.*

Введение. В связи с ежедневно открывающимися фактами прослушивания, слежки в глобальных сетях, проникновения вредоносных программ как в частную жизнь работников предприятия, так и в коммерческую деятельностьсамих предприятий, ни у кого уже не вызывает сомнения в необходимости повышения информационной безопасности (ИБ) предприятия[1]. Организуя комплексную систему защиты информации (СЗИ), поэтапно выстраивая её для конкретного предприятия и выбирая оптимизационный многокритериальный вариант, можно добиться снижения негативных последствий от нарушений ИБ[2].

1. Использование метода моделирования для выбора наилучшего варианта СЗИ. При наличии нескольких, спроектированных для данного предприятия СЗИ, которые оцениваются по разным критериям, и, при этом, оценочные показатели по каждому критерию не совпадают, необходимо прибегать к методу моделирования. Сложность физических систем и многокритериальной оптимизации компенсируется абстрактными описаниями математических моделей. Взаимоотношения реальных физических объектов заменяются символьными отношениями. Устанавливаются правила соответствия между определёнными физическими сторонами объекта и математическими объектами. Рейтингование математических объектов переносится на физические объекты (СЗИ), и задача выбора наилучшего варианта СЗИ проецируется на сравнение координат числовой оси.

При проектировании СЗИ появляются неопределённости стохастического характера, необходимость использования неполной неточной и нечисловой информации (ннн-информации), и принятие оптимизационных решений при неединственности целевой функции. Поэтому целесообразно использовать модифицированный метод рандомизированных сводных показателей (ММРСП).

Метод рандомизированных сводных показателей разработан Хованов Н. В. и Федотовым Ю. В. для исследования сложных объектов при недостатке информации весовых коэффициентов [3],[4].В результате байесовской рандомизации неопределённости, сводные показатели превращаются в соответствующие случайные величины, вычисляются их математические ожидания и дисперсии.

Задача градационного построения объектов сводится к задаче выявления стохастического доминирования между полученными скалярными значениями.

Модификация метода заключается в получении теоретического значения коэффициентаизменения конкурентоспособности, на основе которого происходит рейтингование исследуемых систем.Эксперты оцениваютко эффициент изменения конкурентоспособности $\rho(x)$ для данной СЗИ по шкале критериев, причем минимальное значение является наиболее

предпочтительным.Если k объектов (СЗИ)оценивают по m критериям, токаждая отдельная координата $\rho_i^{(j)}$ является функцией одной исходной характеристики $x_i^{(j)}$: $\rho_i^{(j)}(x_i) j = 1, \dots, k; i = 1, \dots, m.$ Нормирующие функции позволяют перейти к единым единицам измерения $q_i\left(\rho_i(x_i)\right),\ i = 1, \dots, mq \in [0,1]$.Вектор весовых коэффициентов задаёт значимость каждого критерия по отношению к другим $\mathbf{w} - (w_1, \dots, w_m)$, $w_i \geq 0$.Вводится нормировка суммы $w_1 + \dots + w_m = 1$и строится синтезирующая функция $Q^{(j)} = \sum_{i=1}^{m} q_i^{(j)} w_i$.Дискретность модели определяется шагом задания вектора весовых коэффициентов $w_i = \left\{0, \frac{1}{n}, \dots, \frac{n-1}{n}, 1\right\}$,и определяетразмер множества допустимых векторов числовых коэффициентов $N(m,n) = \frac{(n+m-1)!}{n!(m-1)!}$.

Неопределенный выбор вектора весовых коэффициентов из фиксированного множества моделируется случайным выбором из этого множества. Строится аддитивныйрандомизированный сводный показатель $\tilde{Q}^{(j)}(\mathbf{q}, \tilde{\mathbf{w}}) = \sum_{i=1}^{m} q_i^{(j)} \tilde{w}_i$. Получая математическое ожидание $Q^{(j)} = M\tilde{Q}^{(j)}$, мы имеем возможность сравнивать скалярные величины,а мерой градационной точности служит стандартное отклонение $S^{(j)} = \sqrt{D\tilde{Q}^{(j)}}$.Достоверность доминирования сводного показателя $\tilde{Q}^{(m)}$ над $\tilde{Q}^{(l)}$ вычисляется по формуле $P(\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\}) > \alpha$, где $\alpha \in [0,1]$, $m, l = 1, \dots, k.$

При использовании дополнительнойннн-информации I повышается точность оценок весовых коэффициентов, сводных показателей, уменьшаются стандартные отклонения и повышается вероятность доминирования. Сравнивая полученные скалярные величины, мы сравниваем СЗИ, получаем оптимизационный вариант для данного предприятия и теоретическое значение коэффициента изменения конкурентоспособности.

2. Пример применения ММРСП для конкретного предприятия. В период с 2009 г. по 2011 г. на предприятии ООО «Контент-Сервис» был проведен эксперимент по внедрению оптимального варианта СЗИ. Это малое предприятие, занимающееся ремонтом компьютеров и созданием сайтов, состоящее из 9 сотрудников,из которых 8 имеют дело с информационными технологиями. В 2009 г. изучалось предприятие, подбиралась структура и состав будущих СЗИ, службы ИБ. В 2010 г. происходило внедрение.

В 2011 г. изучалась работа предприятия после внедрения СЗИ. В 2012–2013 г.г. обобщались и систематизировались данные эксперимента. На данном предприятии до и после внедрения СЗИ и службы ИБ были проведены анкетирования. Используемые сокращения:

УЭП – доля в процентах участников эксперимента на данном предприятии из всех его сотрудников, применяющих ИТ в своей профессиональной деятельности.

УТП – процент уменьшения тяжелых последствий (по количеству нарушений ИБ) в 2011 г. по сравнению с 2009 г.

УЗП – процент уменьшения заметных последствий (по количеству нарушений ИБ) в 2011 г. по сравнению с 2009 г.

УНП – процент уменьшения незначительных последствий (по количеству нарушений ИБ) в 2011 г. по сравнению с 2009 г.

ПОС – доля в процентах сотрудников - участников эксперимента, положительно оценивающих влияние СЗИ и службы ИБ на свою работу;

ПОЦ – доля в процентах сотрудников - участников эксперимента положительно оценивающих влияние СЗИ и службы ИБ на работу компании в целом.

Таблица 1

Результаты анкетирования ООО «Контент Сервис»

УЭП	УТП	УЗП	УНП	ПОС	ПОЦ
100,0	38,9	24,6	19,8	100,0	100,0

Таблица 1 отражаетдостигнутые положительные результаты при внедрении СЗИ. Более наглядно их демонстрирует следующий график (рис. 1).

На графике указаны проценты уменьшения последствий от количества нарушений ИБ. Все сотрудники, принимавшие участие в эксперименте, считают внедрение СЗИ в компании полезным. Таким образом, можно говорить о том, что произошло усиление ИБ предприятия.

После консультации со специалистами, имеющими дело с информационными технологиями, были получены ущербы, причинённые предприятию вследствие нарушений ИБ. В 2009г. был причинён ущерб в 198 тыс. руб. в год, в 2010г. был причинён ущерб в 162 тыс. руб., в 2011г. был причинён ущерб в 99 тыс. руб. (рис.2).

При выборе СЗИ для данного предприятия было рассмотрено три варианта $(k = 3)$, которые оценивались по трем показателям: целостность, доступность конфиденциальность(m=3).

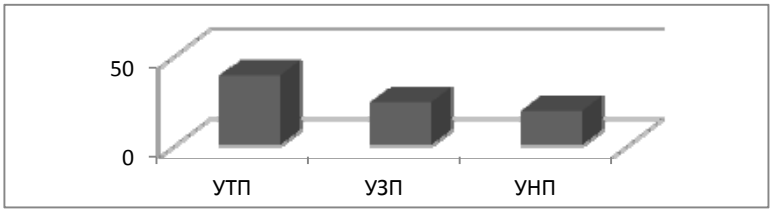


Рис.1. Уменьшение уровня нарушений ИБ ООО «Контент Сервис»

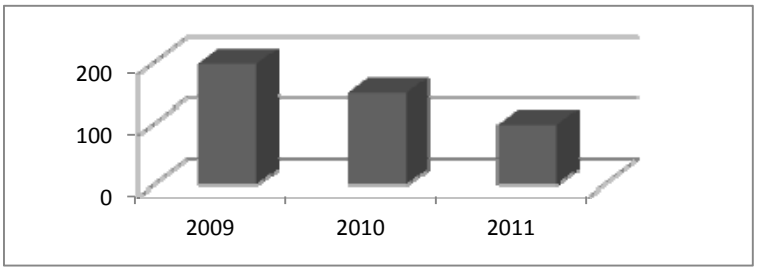


Рис.2. Динамика изменения ущерба по годам компании ООО «Контент Сервис».

Относительная значимость показателей измерялась весовыми коэффициентами w_1, w_2, w_3, а дискретность задавалась шагом $h = \frac{1}{4}$, $n = 4$.Множество векторов весовых коэффициентов $w^{(t)} = (w_1^{(t)}, w_2^{(t)}, w_3^{(t)})$ ограничивается $N(m,n) - 15$ элементами (таблица 2).

Таблица 2

Дискретные значения весовых коэффициентов

$w_3^{(t)}$	1,00	0,75	0,50	0,25	0,00	0,75	0,50	0,25	0,00	0,50	0,25	0,00	0,25	0,00	0,00
$w_2^{(t)}$	0,00	0,25	0,50	0,75	1,00	0,00	0,25	0,50	0,75	0,00	0,25	0,50	0,00	0,25	0,00
$w_1^{(t)}$	0,00	0,00	0,00	0,00	0,00	0,25	0,25	0,25	0,25	0,50	0,50	0,50	0,75	0,75	1,00
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

После опроса экспертов был сформирован вектор $p^{(j)} - (p_1^{(j)}, p_2^{(j)}, p_3^{(j)})$, $j - 1,2,3$.Значения коэффициентов изменения конкурентоспособностисформированы по сетке от 0 до 1 с шагом 0,1 приведены в таблице 3,причем минимальные значения наиболее предпочтительны.

Для унификации значенийпровели линейную нормировку $p^{(j)}$(таблица 4) и получили $q_i(p^{(j)})$

Таблица3

j	$p_1^{(j)}$	$p_2^{(j)}$	$p_3^{(j)}$
1	0,6	0,4	0,6
2	0,5	0,6	0,4
3	0,6	0,5	0,6

Таблица4

j	$q_1^{(j)}$	$q_2^{(j)}$	$q_3^{(j)}$
1	1	0	1
2	0,5	1	0
3	1	0,5	0,5

Подсчитаем значения сводного показателя (табл. 5) трех оцениваемых объектов $j = 1,2,3$.

Таблица 5

Значения рандомизированных сводных показателей

$\tilde{Q}^{(t)}(q^{(1)})$	0,50	0,50	0,50	0,50	0,50	0,625	0,625	0,625	0,625	0,75	0,75	0,75	0,875	0,875	1,00
$\tilde{Q}^{(t)}(q^{(2)})$	0,00	0,25	0,50	0,75	1,00	0,125	0,375	0,625	0,875	0,25	0,50	0,75	0,375	0,625	0,50
$\tilde{Q}^{(t)}(q^{(3)})$	1,00	0,75	0,50	0,25	0,00	1,00	0,75	0,50	0,25	1,00	0,75	0,50	1,00	0,75	1,00
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

В качестве стохастических оценок сравниваемых сводных показателей, вычисляем математические ожидания $\bar{Q}^{(j)} = \frac{1}{N(m,n)} \sum_{t=1}^{N(m,n)} \tilde{Q}^{(t)}(q^{(j)})$.Точность таких оценок определяется стандартными отклонениями $S^{(j)} = \sqrt{\frac{1}{N(m,n)} \sum_{t=1}^{N(m,n)} [\tilde{Q}^{(t)}(q^{(j)}) - \bar{Q}^{(j)}]^2}$ (таблица 6).

Вероятности попарного доминирования рандомизированных сводных показателей приведены в таблице 7.

Таблица 6

j	$\bar{Q}^{(j)}$	$S^{(j)}$
1	0,666	0,186
2	0,5	0,27
3	0,666	0,197

Таблица 7

$P(j,i)$	1	2	3
1	0,000	0,67	0,6
2	0,33	0,000	0,4
3	0,4	0,6	0,000

Все вычисления сделаны при дефиците информации о весовых коэффициентах. Повысить точности вычислений поможет использование дополнительной ннн-информации I. В результате опроса экспертов мы получили $I = \{0{,}25 \le w_1 \le 0{,}75; 0 \le w_2 \le 0{,}50; 0{,}25 \le w_3 \le 0{,}50\}$. Дополнительная информация снижает число возможных числовых коэффициентов до числа допустимых весовых коэффициентов.Редуцированные значения весовых коэффициентов с учетом ннн-информацииприведены в таблице 8.

Число допустимые значения сводных показателей для трех оцениваемых объектов также снижается, что представлено в таблице 9.

Таблица 8

t	$w_1^{(I)}$	$w_2^{(I)}$	$w_3^{(I)}$
1	0,25	0,25	0,50
2	0,25	0,50	0,25
3	0,50	0,00	0,50
4	0,50	0,25	0,25
5	0,75	0,00	0,25

Таблица 9

t	$\bar{Q}^{(I)}(q^{(1)})$	$\bar{Q}^{(I)}(q^{(2)})$	$\bar{Q}^{(I)}(q^{(3)})$
1	0,75	0,375	0,625
2	0,50	0,625	0,625
3	1,00	0,25	0,75
4	0,75	0,50	0,75
5	1,00	0,375	0,875

Математическое ожидание $\bar{Q}^{(I)}(I)$ и стандартные отклонения $S^{(I)}(I)$ подсчитаны с большей точностью и приведены в таблице 10.

Вероятности попарного доминирования $P(j, l)(I)$ возрастают, что показано в таблице 11.

Таблица 10

j	$\bar{Q}^{(I)}(I)$	$S^{(I)}(I)$
1	0,8	0,147
2	0,425	0,125
3	0,725	0,071

Таблица 11

$P(j, l)(I)$	1	2	3
1	0,00	0,80	0,60
2	0,20	0,00	0,00
3	0,40	1,00	0,00

Учет ннн-информации уменьшает стандартные отклонения и увеличивается достоверность рейтингования. Мы выбираем СЗИ с наименьшим математическим ожиданием, небольшим стандартным отклонением и большой достоверностью рейтингования.Получается второй вариант СЗИ.Математическое ожидание $\bar{Q}^{(I)}(I) = 0{,}425$ выбранной СЗИ мы проецируем на первоначальную оценочную шкалу экспертов(табл. 3) и получаем значение коэффициента изменения конкурентоспособности для данной СЗИ $\mu(x) = (0{,}6 - 0{,}4) \cdot 0{,}425 + 0{,}4 = 0{,}485$.После внедрения СЗИ и получения данных о снижении ущербов от нарушения ИБ, можно сосчитать реальное значение коэффициента изменения конкурентоспособности $\mu_{реал} = \frac{У_{реал}}{У_{2007}} = \frac{99}{199} = 0{,}5$.Можно сделать вывод, что теоретические результаты оказались близки к реальным. После внедрения оптимизационного варианта СЗИ, произошло усиление ИБ и полученное теоретическое значение коэффициента изменения конкурентоспособности можно использовать для подсчёта количественного значения конкурентоспособности предприятия[5],[6].

Заключение. Предложено решение выбора СЗИ на основе ММРСП.Проведено внедрение выбора оптимального варианта СЗИ на предприятии ООО «Контент-Сервис». Итогами внедрения стали усиление ИБ и уменьшение ущерба предприятию. Полученное модельное значение коэффициента изменения конкурентоспособности может в дальнейшем использоваться для подсчёта конкурентоспособности предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Левкин И.М., Левкина С.В., Сорокина Е.А. Информационно-признаковое моделирование угроз национальной безопасности// Вестник Академии военных наук. Северо-Западное отделение, 2013.
2. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб: БХВ–Петербург, 2003. 752 с.: ил. ISBN 5 – 94157 – 280 – 8 УДК 681.3.06 ББК 32.973. К64
3. Хованов Н.В., Федотов Ю.В. Модели учета неопределенности при построении сводных показателей эффективности деятельности сложных производственных систем № 28(R)-2006. СПбГУ Научно-исследовательский институт менеджмента научные доклады [Электронный ресурс]. Режим доступа: http://dspace.gsom.pu.ru/jspui/bitstream/123456789/91/1/28%28R%29_2006.pdf, свободный. Яз.рус. (дата обращения 09.02.14).
4. Hovanov N., Yudaeva M., Hovanov K.Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge // Abstracts of 18-th International Conference on Multiple Criteria Decision Making. Chania (Greece), June 19-23, 2006. P.102.
5. Попова Е.В. Расчет конкурентоспособности малых предприятий сферы сервиса при усилении информационной безопасности // Журнал «Вестник российской академии естественных наук». Сентябрь 2012, 16(3): С. 48–51.
6. Левкин И.М., Микадзе С.Ю. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе// VIII Санкт-Петербургская межрегиональную конференцию «Информационная безопасность регионов России (ИБРР-2013)», 2013.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ

УДК 681.5

ЭФФЕКТИВНЫЙ МЕТОД ГРУППОВОЙ НАВИГАЦИИ, ОСНОВАННЫЙ НА МОДИФИЦИРОВАННОМ АЛГОРИТМЕ А*

Ерохин Александр Владимирович[1], Ерохин Владимир Иванович[2],
[1] ФГАНУ «ЦНИИ РТК»,
Россия, Санкт-Петербург, Тихорецкий пр. 21,
[2] Санкт-Петербургский государственный технологический институт (технический университет),
Россия, Санкт-Петербург, Московский пр. 26,
e-mails: erohin_v_i@mail.ru

Аннотация: Рассмотрен алгоритм построения маршрутов для группы мобильных роботов, оснащенных датчиками сканирования пространства и определения относительного положения членов группы, основанный на модифицированном алгоритме А*. Приведены результаты вычислительных экспериментов на картах различного типа и для различной численности группы роботов.

Ключевые слова: *нахождение пути; построение маршрута; группа роботов; моделирование*

EFEECTIVE MULTI-ROBOT NAVIGATION METHOD, BASED ON A* PATH-FINDING ALGORITHM MODIFICATION

Alexander Erohin[1], Vladimir Erohin[2],
[1] Russian state scientific center for robotic and technical cybernetics,
Russia, St. Petersburg, Tikhoretsky prospect 21,
[2] Saint-Petersburg State Institute of Technology (Technical University),
Russia, St. Petersburg, Moskovsky prospect 26,
e-mails: erohin_v_i@mail.ru

Abstract: Path finding method for a group of mobile robots, equipped with scanning sensors and sensors capable of determining relative positions of robots, based on A* algorithm is presented. Results of computer experiments on maps of different types and for different group count are given.

Keywords: *path finding; route planning; group of robots; computer modeling*

Введение. Задача навигации и управления автономными мобильными устройствами является фундаментальной проблемой робототехники [1], [2]. В последнее десятилетие наибольшее внимание робототехнического сообщества было уделено разработке методов управление движением группы мобильных роботов, так как группа содержит потенциал решения задач, с которыми единственное устройство не в состоянии справиться или справляется неэффективно [3]. В область интереса групповой робототехники входят такие задачи как: погрузка или транспортировка грузов, патрулирование, поисковые и спасательные работы, работы исследовательского характера, покрытие и составление карт неизвестных или мало известных территорий и многое другое.

Использование группы роботов имеет большое количество преимуществ. Наиболее важными из них являются: уменьшение длины пути или времени выполнения задания и увеличение надежности, так как выход из строя одного или нескольких членов группы не должен сказаться на ее работе в целом за счет избыточности группы, что позволит выполнить задание. Уменьшение индивидуальной механической нагрузки и энергетических затрат увеличивает срок службы каждого робота. Поддержание связи и обмена информацией между членами группы уменьшает неопределённость данных сенсорных устройств, ввиду перекрытия областей сканирования.

В настоящей работе будет предложен и описан новый эффективный метод групповой навигации, основанный на модифицированном алгоритме А*. Кроме того будут приведены результаты тестирования метода на картах местности различного типа.

Постановка задачи. Имеется группировка мобильных роботов, оснащенная датчиками сканирования пространства и определения относительного положения членов группы. Стоит задача осуществления перемещения из начального положения в заданное конечное всех членов группы по

неизвестной карте. Поставленная задача считается решенной, если все члены группы роботов достигают некоторой окрестности заданного конечного положения. Окрестность определяется габаритами роботов и численностью группы. Задача считается неразрешимой, если в ходе построения карты выясняется, что точка назначения и ее окрестность лежат вне досягаемой области.

Для дальнейшей формализации задачи примем ряд допущений, связанных с конфигурацией мобильных роботов, и рассмотрим ряд вспомогательных задач, определяющих алгоритмы их взаимодействия.

Допущения:

1. Предполагается, что группой роботов ведется общая карта местности. Эта карта уточняется по мере передвижения роботов и доступна для каждого члена группы;
2. Задание конечного положения осуществляется относительно начального положения роботов и доступно для всех членов группы.

Разработка алгоритма навигации. За основу разрабатываемого алгоритма был взят алгоритм нахождения пути A*. Отмеченный за свою производительность и точность алгоритм получил очень широкое распространение. Кроме того, на основе этого алгоритма уже создано достаточно большое количество модификаций [4], [5], направленных на решение задач в различных областях прикладных знаний, но выигрывающих в эффективности благодаря полезным свойствам оригинального алгоритма.

Напомним, что алгоритм A* использует в своей основе поиск по первому наилучшему совпадению и находит путь наименьшей стоимости из текущего узла в заданный конечный. При выполнении алгоритма во время прохождения по графу выстраивается путь с наименьшей ожидаемой стоимостью прохождения. Порядок обхода вершин определяется эвристической функцией «расстояние + стоимость» (обычно обозначаемой как $f(n)$). Эта функция — сумма двух других: функции стоимости достижения рассматриваемой вершины n из начальной (обычно обозначается как $g(n)$ и может быть как эвристической, так и нет) и эвристической оценкой расстояния от рассматриваемой вершины к конечной (обозначается как $h(n)$).

Первоочередная задача, которую необходимо решить – расширение области применения алгоритма до группы роботов, совершающих движение к единой цели. Рассмотрим трудности, которые при этом возникают. Во-первых, наличие общей карты подразумевает доступ к ней всех членов группы. То есть возникает необходимость обеспечения целостности данных об узлах карты (в нашем случае: весах, проходимости и прочего). Во-вторых, возникает необходимость контроля пересечения маршрутов в целях исключения одновременного использования одного и того же узла несколькими роботами, таким образом предотвращения возможных столкновений. В-третьих, с новой стороны встает вопрос эффективности поиска маршрута для группы роботов, когда становится необходимо обеспечить эффективное передвижение как группы в целом, так и каждого отдельного робота.

Целостность данных может быть обеспечена разграничением доступа членов группы к общей карте. При этом порядок доступа может определяться в зависимости от приоритета члена группы или приоритета операции над общими ресурсами. Проблемы же пересечения маршрутов и эффективности рассчитываемых путей могут быть решены путем модификации исходного алгоритма A* таким образом, чтобы учитывались специфические условия задачи.

Существуют некоторые известные и находящие свое применение в различных алгоритмах пути исключения коллизий между перемещающимися объектами [6]. Общий недостаток существующих подходов заключается в необходимости введения дополнительной информации или флагов для предотвращения столкновений. В рассматриваемом далее решении предлагается использовать существующую информацию об узлах для предотвращения коллизий.

Итак, пусть имеется некоторая функция $\tilde{f}(n)$, определяющая фактическую стоимость оптимального пути из s в a, проходящего через n. Тогда $\tilde{f}(n)$ может быть представлена в виде суммы двух функций:

$$\tilde{f}(n) = \tilde{g}(n) + \tilde{h}(n), \tag{1}$$

где $\tilde{g}(n)$ определяет фактическую стоимость оптимального пути из s в n;

$\tilde{h}(n)$ определяет фактическую стоимость оптимального пути из n в a.

В виду того, что $\tilde{f}(n)$ является априори неизвестной, приемлемо воспользоваться приближением $\tilde{f}(n)$ оценочной функции $f(n)$. Если задаться кроме этого приближениями $\tilde{g}(n)$ и $\tilde{h}(n)$, получим:

$$f(n) = g(n) + h(n) \tag{2}$$

Здесь предполагается, что слагаемое $g(n)$ является некоторой характеристикой цены перехода к данному узлу от начального. В рамках рассматриваемой задачи движения такой характеристикой может выступить время, затрачиваемое на прохождения узла. Таким образом цена перехода от узла к узлу по диагонали будет больше цены перехода по вертикали или горизонтали ввиду больших временных затрат на движение. Кроме того, такая характеристика цены позволяет учитывать эффективность проложенных маршрутов.

Пусть, в силу обеспечения целостности данных, расчет пути членов группы осуществляется последовательно в порядке очереди. Тогда к весу узлов, уже входящих в пути членов группы, целесообразно прибавлять постоянную поправку C_n в виде некоторого слагаемого постоянного по модулю. Таким образом, гарантированно получаем:

$$g(n) \geq \tilde{g}(n) \tag{2}$$

Постоянная поправка C_n будет означать следующее: «этот узел уже входит в путь одного или нескольких членов группы; если очередной член решит использовать узел – возможна ситуация того, что в момент прохождения пути узел будет занят и придется ждать». В рамках алгоритма такой узел прибавит в цене в смысле времени, и может оказаться так, что в процессе расчета пути «дешевле» будет выбрать путь, который идет в обход занятых узлов, вместо того, чтобы стоять в очереди на их доступность [7].

Для сокращения числа рассматриваемых узлов необходимо определиться со значением эвристической составляющей функции оценки веса узла.

Согласно теореме [8, Theorem 1], при (2) и $h(n) \geq \tilde{h}(n)$ алгоритм является приемлемым в том смысле, что обеспечивает нахождение оптимального пути. Таким образом, пока $h(n)$ не переоценивает фактическое расстояние до цели – найденный путь будет гарантированно оптимальным. Таким образом, наша оценка $h(n)$ может иметь значение

$$h(n) = \sqrt{\Delta x^2 + \Delta y^2}\ , \tag{3}$$

где Δx и Δy – значения разностей координат x и y текущего узла и узла назначения, являющегося прямым расстоянием до конечного узла без наличия препятствий.

Тогда в результате работы алгоритма все равно будет найден оптимальный путь, но при этом исследовано меньшее количество узлов. С другой стороны, может получиться так, что вычислительные затраты на подсчет (3) могут оказаться значительными, по сравнению с исследованием дополнительных узлов. То есть оптимальная процедура в смысле исследования минимального количества узлов может оказаться не оптимальной в смысле общего минимального задействования ресурсов. В таком случае может быть выбрана оценка:

$$h(n) = \frac{|\Delta x| + |\Delta y|}{2} \tag{4}$$

Так как $\frac{|\Delta x| + |\Delta y|}{2} < \sqrt{\Delta x^2 + \Delta y^2}$ алгоритм все равно остается приемлемым. Так как в данном случае используется не вся известная информация об области задачи, некоторое дополнительное количество узлов может быть исследовано, но общие вычислительные затраты при этом будут уменьшены.

Следующей задачей после расширения области применения алгоритма на группу роботов является задача неполноты данных. Изначально группе роботов неизвестна местность, по которой происходит движение. Карта местности компилируется по ходу движения на основе данных, получаемых с бортовых датчиков мобильных роботов. Таким образом, возможна ситуация, при которой пути, рассчитанные на одном из этапов движения, могут оказаться непроходимыми при компиляции карты по новым данным на следующем этапе.

Таким образом, встает задача перерасчета путей членов группы с учетом ново полученной информации с датчиков сканирования пространства, установленных на борту роботов. Необходимо понимать, что частые перерасчеты маршрутов следования могут негативно сказаться на быстродействии алгоритма и загрузке расчетных модулей роботов. С другой стороны, недостаточно частые корректировки могут привести к неадекватному обстановке исполнению команд роботами. На основе представленных соображений, для целей моделирования было решено осуществлять пересчеты маршрутов после внесения новый информации на карту любым из членов группы, при условии того, что хотя бы один из рассчитанных путей пересекает новый непроходимый участок. Таким образом, был достигнут некоторый компромисс между быстродействием и точностью.

Итак, пусть s – начальное стартовое положение, T – множество точек, отвечающее за положение цели. Определим алгоритм поиска пути для группы агентов в виде пошаговой процедуры,

выполняемой последовательно для каждого агента, возвращаемым значением которого является список узлов, входящих в путь.

Модифицированный алгоритм поиска A*.

1. Пометить s как открытый узел и вычислить $f(s)$.

2. Выбрать из списка открытых узлов узел n, чье значение $f(s)$ минимально. Ситуации с совпадением значений $f(s)$ разрешать случайным образом, но всегда в пользу узлов $n \in T$.

3. Если $n \in T$, добавить n в список закрытых узлов. Сохранить путь P, двигаясь назад от целевого узла к его родителю, пока не будет достигнут стартовый узел s. Для каждого узла $n \in P$ увеличить постоянную составляющую $g(n)$ на некоторое значение C_n. Закончить выполнение алгоритма для данного агента.

4. В противном случае поместить n в список закрытых узлов. Для каждого из восьми соседних узлов n_i сделать следующее:

а. если узел n_i непроходим или находится в закрытом списке, игнорировать его;

б. если узел n_i еще не в открытом списке, добавить его туда. Сделать текущий узел родительским для этого узла. Рассчитать $h(n_i)$ и $g(n_i)$ узла с учетом постоянной поправки NC_n, где N – количество агентов, использующих данный узел в пути;

в. если узел уже находится в открытом списке, проверить, не дешевле ли путь через данный узел. Для сравнения использовать значения $g(n_i)$. Если $g(n_i) < g(n_i')$, то есть путь оказался дешевле: заменить родителя узла на текущий узел, пересчитать значения $h(n_i)$ и $g(n_i)$ узла с учетом постоянной поправки NC_n.

5. Перейти к шагу 2.

Оценка результатов работы и выводы. Заключительным этапом разработки являлась оценка результатов работы алгоритма. Для получения большей и более полной выборки результатов тестирование работы алгоритма проводилось для различных типов конфигурации карт и различной численности группы роботов.

Разобьем всевозможные конфигурации карт местности на следующие два типа:

1. Карты открытого типа;
2. Лабиринты.

К картам открытого типа будем относить карты, препятствия на которых имеют локальный характер, а проходы между ними больше или соизмеримы с размерами самих препятствий и много больше размеров роботов. К таким картам можно отнести, например, карту офисного помещения или склада «Рисунок 1», где стеллажи или рабочие места, выступающие в роли препятствий, оставляют довольно просторные связанные между собой проходы. В виду обширных открытых территорий такие карты оставляют большее пространство для маневра, а так же быстрее поддаются исследованию с помощью датчиков роботов.

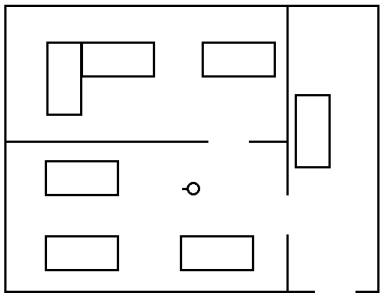


Рис. 1. Пример открытой карты

С другой стороны, к лабиринтам «Рисунок 2» отнесем карты, препятствия на которых имеют протяженную форму и соединяются между собой. Свободные области представлены, в основном, коридорными участками, ширина которых сопоставима с размерами робота.

В качестве показателя результатов работы может быть выбрано количество законченных шагов движения до достижения всеми членами группы заданной окрестности цели. Такой показатель легко поддается подсчету и при постоянном времени шага движения может выступать в качестве оценки затрачиваемого времени. Было так же решено на всех типах карт осуществлять моделирование для

групп численностью 5, 10 и 15 роботов. Кроме того на каждой отдельной карте предусматривалась сессия моделирования прохождения до цели единственного робота. Измерение количества шагов, необходимого одиночному роботу на нахождения цели, позволяет провести анализ эффективности передвижения группы роботов разной численности по той же карте.

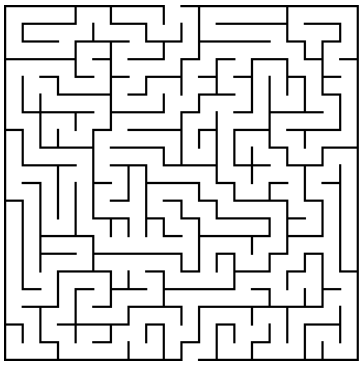


Рис. 2. Пример лабиринта

По результатам моделирования можно сделать следующие выводы. Хорошие результаты на открытой карте демонстрируют одиночные роботы. Связано это с тем, что большинство препятствий находятся в прямой видимости сканирующих устройств, что позволяет уже после начального сканирования построить путь до цели близкий к оптимальному.

Кроме того открытость карты позволяет избежать частых перестроек пути. По мере увеличения численности группы происходит увеличение количества шагов, необходимых для достижения всеми членами группы цели. Объяснить такие приросты относительно единичного робота можно наличием на картах выделенных оптимальных маршрутов достижения цели, полностью доступных для одного робота, но являющихся объектом конкуренции группы.

Обратная картина наблюдается при работе алгоритма на картах типа лабиринт. Относительно большое количество шагов понадобилось в обоих случаях единичному роботу для преодоления карты. Это можно объяснить большим количеством проходов, ведущих в тупики. На картах такого типа проявляется ряд факторов, ограничивающий возможности сбора информации, а так как единственный робот вынужден руководствоваться информацией, полученной исключительно со своих измерительных устройств, большое количество шагов тратиться как раз на исследование окружающей среды. С другой стороны, при увеличении численности группы роботов уменьшается количество шагов, необходимое для преодоления карты группой.

Действительно, при увеличении группы увеличивается количество собранной информации на каждом шаге движения.

Таким образом, происходит параллельное исследование карты и поиск маршрута до цели. В отличие от открытой карты, где цель находилась в прямой видимости некоторых членов группы практически с первых шагов движения, на картах типа лабиринт цель попадает в видимость только при ее достижении. Увеличение числа роботов соответственно увеличивает и вероятность нахождения пути до цели.

Однако, при дальнейшем увеличении численности группы наблюдается эффект перенасыщения карты роботами. Слишком большое количество агентов приводит к нехватке альтернативных направлений движения в рамках лабиринта, что снижает эффективность работы каждого робота. На каждый возможный маршрут приходится более одного робота, а повторные прохождения уже пройденных другими членами узлов не несут полезной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Юревич Е.И.. Основы робототехники. – 2-е изд., перераб. и доп. – СПб.: БХВ–Петербург, 2005. – 416с.
2. M.C. Hoy. Methods for collision-free navigation of multiple mobile robots in unknown cluttered environments // Cornell University. – 2014.
3. A. Fujimori, H. Kubota, N. Shibata, Y. Tezuka. Leader-follower formation control with obstacle avoidance using sonar-equipped mobile robots // Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering. – 2014. – p. 1 – 13.
4. A. Das, P. Mohapatra, P. Mishra, P. K. Das, S. C. Mandhata. Improved real time A* algorithm for path planning of mobile robot in quadrant based environment // International Journal on Advanced Computer Theory and Engineering. – 2012. – P. 7 – 12.
5. A. Botea, M. Muller, J. Schaeffer. Near optimal hierarchical path-finding // Journal of Game Development. – 2004.
6. S. Vincke. Real-time pathfinding for multiple objects // Game Developer. – 1997. – P. 36 – 44.
7. Ерохин А.В., Ерохин В.И. Алгоритм группового самоуправления коллектива роботов при построении пути к цели с учетом препятствий по неизвестной карте на основании данных сканирования пространства и определения относительного положения членов группы (тезисы) // М-лы научн. конф., посвященной 185-й годовщине образования СПбГТИ(ТУ). – Изд.-во СПбГТИ(ТУ). 2013. С. 259.
8. P. Hart, N Nilsson, B. Raphael. A formal basis for the heuristic determination of minimum cost paths // Transactions of Systems Science and Cybernetics, Vol. ssc-4. – NO. 2 – July 1968. – p. 100 – 107.

УДК 681.391

СОПОСТАВЛЕНИЕ ДВУХ МЕТОДОВ АВТОМАТИЧЕСКОЙ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ

Ханыков Игорь Георгиевич,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия В.О., д.39,
e-mail: igk@iias.spb.su

Аннотация: Задачи выделения объектов на изображениях в системах компьютерного зрения решаются при помощи методов сегментации. Существующие методы сегментации изображения строятся по схеме выделения целевого объекта по его априори заданным ключевым признакам. Эти решения эффективны, но узкоспециализированы. Возникает актуальная задача разработки универсального инструмента сегментации, выполняющего автоматическую сегментацию без априорной информации о содержании изображения. В данной работе рассматриваются два метода автоматической сегментации изображения: метод адаптивной сегментации изображения по цвету и текстуре, и метод построения кусочно-постоянных приближений сегментированного изображения.

Ключевые слова: *цветовая и текстурная сегментация, кусочно-постоянное приближение, доминирующие цвета, среднеквадратическое отклонение, минимизация*

TWO METHODS OF AUTOMATIC IMAGE SEGMENTATION COMPARISON

Khanykov Igor Georgievich,
St.Petersburg Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line, 39,
e-mail: igk@iias.spb.su

Abstract*:* The objects allocation problems in the images in the computer vision systems are solved by means of segmentation methods. The existing image segmentation methods are developed aiming to isolate target object by its a priori given key features. Such solutions are effective, but highly specialized. Here rises the relevant objective of the universal segmentation toolkit development, which is able to carry out «blind segmentation» without the aprioristic information about the image content. Current paper considers two blind image segmentation **methods**: Method of adaptive image segmentation based on color and texture and Segmentation method based on piecewise-constant approximations.

Keywords: *color and texture segmentation, piecewise-constant approximation, dominant colors, standard deviation, minimization*

Введение. Компьютерное зрение – это одно из направлений компьютерной науки информатики и кибернетики. Конечная цель компьютерного зрения – создание инструмента искусственного зрения, включающего в себя систему обучения, анализа, принятия решения на основе входного цифрового видеопотока данных.

Компьютерное зрение применяется в различных областях народного хозяйства, индустрии, в военном деле и в научных исследованиях. Например, в медицине наблюдение за состоянием внутренних органов помогает установить диагноз пациента. В военном деле снятие и обработка аэрокосмических снимков служит нуждам мониторинга обстановки. В промышленности средства компьютерного зрения поддерживают производственный процесс (контроль качества, измерение положения и ориентации деталей и др.). В автомобилестроении актуальны перспективы внедрения автопилота в бортовую компьютерную систему автомобиля. В охранных системах самый распространенный вид контроля – это видео мониторинг. Уже созданы и успешно внедряются программно-аппаратные комплексы трекинга объектов, распознавания лиц и систем контроля дорожного движения.

Востребованность систем компьютерного зрения подчеркивает значимость задачи выделения объектов на изображении – сегментации изображения. Существующие сегментационные решения строятся по схеме выделения целевого объекта (текста, лиц, и пр.) по его априори заданным ключевым признакам. Однако, каждое отдельное решение является узконаправленным и имеет ограниченные возможности распознавания объектов. Получаемые на выходе эффективные, но частные решения создаются за счет трудоемкого программирования и предварительного обучения системы на объектах «интереса». Возникает актуальная задача разработки универсального инструмента сегментации, выполняющего сегментацию «вслепую» без априорной информации о содержании изображения.

В работе рассматриваются решения автоматической сегментации в применении кластерного анализа, полагая процессы выделения и распознавания объектов раздельными, но следующими друг за другом. Выполняется сопоставление двух методов слепой сегментации изображения: метод

адаптивной сегментации изображения по цвету и текстуре, и метод построения кусочно-постоянного приближения сегментированного изображения.

Метод адаптивной сегментации изображения по цвету и текстуре

В работе [1] предлагается метод сегментации изображения на основе объединения текстурных и цветовых признаков, поэтапная схема которого представлена на рисунке 1. На начальном этапе выполняется вычисление первых и вторых признаков. Затем грубое промежуточное решение (приближение) последовательно улучшается. Таким образом, цветовая и текстурная сегментация дополняют друг друга.

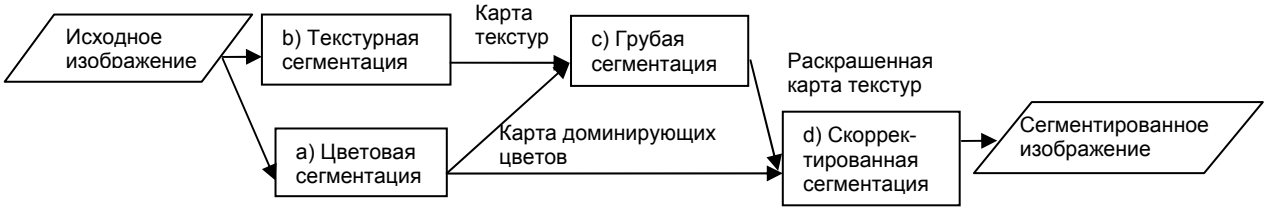


Рис. 1. Поэтапная схема адаптивного алгоритма сегментации изображения

a) Цветовые признаки. Сегментация по цвету. Для проведения цветовой сегментации необходимо предварительно извлечь цветовые признаки. В качестве цветовых признаков используется компактное цветовое представление в терминах доминирующих цветов, которое было впервые предложено в работе [2] и записывается в векторном виде:

$$f_c = \{(c_i, p_i); i = 1,...,N; p_i \in [0,1]\}.$$

где c_i – *RGB*-вектор доминирующих цветов, p_i – относительное присутствие цвета в области.

Существует ряд способов получения такого представления.

Первый способ – применение алгоритма Команицу-Мейера (Comaniciu-Meer, CM) [3], к преимуществам которого относится простота и эффективность получения признаков доминирующих цветов изображения любого тематического содержания, а недостатком – образование ложных контуров. Для обхода этого недостатка в работе [1] используется *пространственно-адаптивные доминирующие цвета*, учитывающие вариацию характеристики на протяжении изображения.

Второй способ – извлечение цветовых признаков по адаптивному алгоритму кластеризации (Adaptive Clustering Algorithm, ACA), предложенному в [4] и усовершенствованному для цветного изображения в [5]. На выходе ACA получают разбиение исходного изображения на области, каждой из которых соответствует свой вектор доминирующих цветов. В пределах окрестности значение цвета считается постоянным. Затем, полученные области изображения и соответствующие им вектора доминирующих признаков связываются по критерию оптимального расстояния цветовой композиции «OCCD» [6]. Вычисление критерия сводится к оптимизационной задаче поиска минимальной «стоимости» графа. Если задан набор узлов, а дуги ассоциируются с затратами, то задача построения графа *минимальной стоимости* сводится к проблеме поиска набора раздельных дуг с минимальной общей стоимостью (у дуг нет общих узлов). В данной задаче узлами выступают элементы векторов доминирующих цветов, а стоимости сочетания пар цветов задается заранее в кодовой книге цветов.

b) Текстурные признаки. Текстурная сегментация. В работе [1] предлагают использовать ограниченный набор типов текстур («вертикальная», «горизонтальная», «гладкая», «сложная») и отказаться от детального распознавания каждой области изображения.

В качестве текстурных признаков используются *энергетические коэффициенты*, извлекаемые при помощи сепарабельного биортогонального одноуровневого 9/7 вейвлет-разложения [7]. Для подчеркивания границы и исключения плавных переходов используется медианный оконный оператор 9x9. «Сборка» текстурных сегментов одного типа осуществляется посредством двухуровневого *K-means* алгоритма [8].

После того, как по раздельно найденным текстурным и цветовым признакам построены соответствующие разбиения, 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.

c) Грубая сегментация. На этапе «раскраски» грубой сегментации раздельно обрабатываются сегменты «гладких» текстурных областей и все остальные. Этап подразделяется на блоки операций.

В первом блоке операций рассматриваются только «гладкие» текстурные области и, опираясь на цветовую сегментацию, принимается решение, следует ли текстурные области далее подразделять на сегменты различных цветов, что описывается следующим образом:

1. Для каждой связанной «гладкой» текстурной области (*connected smooth region*):

– находятся все связные (*connected segments*), но принадлежащие различным классам цветов, сегменты и вычисляются их средние значения цветов;

– объединяются цветовые сегменты, чьи цвета близки.

2. Для оставшихся цветовых сегментов:

– вычисляются средние разницы по общей границе;

– сегменты объединяются, если разница в цвете меньше пороговой величины.

Все мелкие «гладкие» текстурные области, граничащие с «не гладкими», рассматриваются во следующем блоке операций. При этом рассматриваются все оставшиеся текстурные области, и выполняется процедура объединения областей, параметрами которой являются ранее определенные текстурные и цветовые признаки, а именно, карта текстур из оттенков серого, а также вектора доминирующих цветов с их привязкой к изображению.

Для каждой пары пикселей:

– вычисляется разница цветовых признаков по критерию OCCD;

– выполняется объединение, если разница не превышает заданного порога.

d) Скорректированная сегментация. На этом этапе «коррекции» грубой сегментации выполняются операции по уточнению границы сегментов посредством перераспределения пограничных пикселей между смежными цветовыми сегментами для получения результирующей сегментации.

Для каждого пикселя вдоль границы грубой сегментации:

– сравнивается значение цвета пикселя, полученного алгоритмом ACA, со средними значениям цветов смежных сегментов по обе стороны границы;

– пиксель перемещается в тот цветовой сегмент, чье среднее значение цвета ближе всего к значению рассматриваемого пикселя.

Операция «коррекции» не производится, если значения цветов смежных областей достаточно близки.

Метод построения кусочно-постоянных приближений сегментированного изображения

Предлагаемый в работе [9] и развиваемый в [10] метод автоматической сегментации цифровых изображений посредством кусочно-постоянных приближений относится к области применения классического кластерного анализа. Модель состоит в следующем:

1. Полагается, что изображение состоит из вложенных «объектов», которые сами являются изображениями.

2. Вложенный «объект» образуют усредненные по яркости (цвету) пиксели. При сегментации вложенный «объект» формируют только смеженные пиксели. При кластеризации «объекты» объединяются в множества несмежных сегментов. Образованное из таких объектов изображение называется *кусочно-постоянным приближением*. Под *суперпикселями* понимают связные сегменты изображения, не содержащие границ зрительно воспринимаемых объектов.

3. На выходе задачи сегментации получают разбиения с числом сегментов (кластеров) существенно меньшим числа пикселей N.

4. Качество разбиения и соответствующего *приближения* изображения численно оценивается по среднеквадратичному отклонению σ приближения от изображения или суммарной квадратичной ошибке [11].

5. Поскольку определение последовательности оптимальных приближений от 1 до числа N пикселей изображения из-за высокой вычислительной сложности. Поскольку задача является *NP*-трудной, эту последовательность аппроксимируют иерархическими квазиоптимальными приближениями.

6. В методе сегментации кусочно-постоянными приближениями [9, 10] построение иерархии квазиоптимальных разбиений предлагается выполнять в три этапа, которые схематично представлены на рисунке 2.

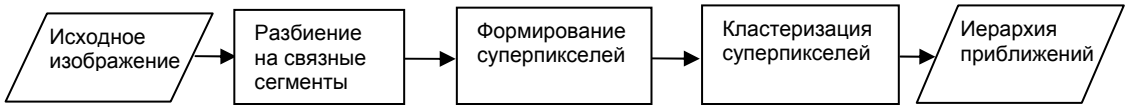


Рис. 2. Последовательная схема вычислений

Рисунок 2 включает в себя следующие блоки:

– разбиение изображения на связные сегменты выполняется в модели Мамфорда-Шаха [12–15];

– суперпиксели формируются в алгоритмах улучшения качества сегментации [16];

– кластеризация суперпикселей производится методом Уорда [17].

7. Инструментарий модели иерархической сегментации [18, 19] образуют четыре операции, которые минимизируют суммарную квадратичную ошибку *E* или среднеквадратичное отклонение σ:

– операция «merge» слияния двух кластеров;
– операция «divide» разделения кластера надвое;
– операция «split» выделения части кластера в отдельный кластер;
– операция «correct» реклассификации пикселей.

Первые две операции с кластерами пикселей и сегментами изображения используются при построении и обработке модифицируемой или фиксированной иерархии кластеров. Пара остальных операций используется при построении и преобразованиях иерархии. На первом и заключительном этапах получения иерархии вычисления сводятся к итеративному слиянию множеств пикселей из условия минимизации приращения суммарной квадратичной ошибки.

a) Разбиение изображения на связные сегменты в модели Мамфорда-Шаха.

На первом этапе разбиение изображения выполняется в модели Мамфорда–Шаха посредством перебора ограниченного множества пар смежных сегментов, что хотя и влечет некоторое увеличение ошибки E аппроксимации изображения по сравнению с методом Уорда [17], [18], но при этом снижает вычислительную сложность до линейной зависимости от числа N пикселей в изображении и обеспечивает аппроксимацию изображения любым числом связных сегментов от 1 до N.

b) Формирование суперпикселей в алгоритмах улучшения качества.

В случае иерархии сегментов изображения сочетание операций «*merge*&*divide*» обеспечивает улучшение качества приближения изображения на втором этапе за счет итеративного разделения надвое одного из сегментов и слияния несовпадающих с ним двух других по критерию минимизации суммарной квадратичной ошибки.

c) Кластеризация суперпикселей методом Уорда.

Метод Уорда гарантированно обеспечивает минимум приращения суммарной квадратичной ошибки, но поскольку вычислительная сложность метода Уорда квадратично зависит от числа пикселей N, то целесообразно редуцировать входное множество, что успешно выполняется на предшествующих этапах **a** и **b**. Алгоритмически этап **c** подобен этапу **a** с той лишь разницей, что конечная иерархия образуется путем слияния всевозможных пар укрупненных областей.

В сравнительной таблице сопоставляются основные положения двух методов слепой сегментации.

Таблица 1

Сравнительная таблица двух методов слепой сегментации

Метод	**Метод сегментации на основе текстурных и цветовых признаков**		**Метод кусочно-постоянных приближений**
Модель	Объединение алгоритмов текстурной и цветовой сегментации		Изображение из «объектов»; Иерархия кусочно-постоянных приближений; Алгоритмы кластерного анализа;
	Цветовая сегментация	Текстурная сегментация	
Признаки	Коэффициенты векторов доминирующих цветов	Энергетические коэффициенты	Яркости пикселей
Критерий объединения	min{ OCCD }	Порог детектирования доминирующего цвета	Минимизация среднеквадратичного отклонения
Вычислительный аппарат	Извлечение признаков - Адаптивный алгоритм кластеризации (ACA) Сборка по критерию объединения	1. Извлечение признаков – сепарабельное одноуровневое 9/7 вейвлет-разложение; 2. Унификация окрестности границ сегментов медианным оператором 9x9 3. Сборка текстур одного типа – двухуровневый K-means	1. Модель Мамфорда-Шаха, 2. Метод Уорда, *3. K-meanless,* Операции над кластерами пикселей и сегментами изображения *Merge, Divide, Split, Correct*
Вычислительная сложность	OCCD: кубическая сложность ACA: кубическая сложность	1. Линейная сложность 2. Линейная сложность 3. Квадратичная сложность	1. Линейная сложность 2. Квадратичная сложность 3. Квадратичная сложность

Заключение. Одна из актуальных задач компьютерного зрения – создание унифицированного сегментатора, т.е. инструмента выделения объектов изображения без априорной информации о содержании изображения. В данной работе рассмотрены два метода сегментации: метод адаптивной сегментации изображения по цвету и текстуре, и метод построения кусочно-постоянных приближений сегментированного изображения. Основное преимущество рассмотренных методов в том, что они относятся к классу методов автоматической сегментации. В работе раскрыты основные алгоритмы каждого метода:

1. В обоих методах проблема вычислительной сложности при кластеризации обходится путем рассмотрения ограниченного набора входных множеств данных. В методе сегментации по цвету и

текстуре адаптивный алгоритм кластеризации обеспечивает извлечение цветовых признаков ограниченных по площади областей изображения. Затем по критерию оптимального расстояния цветовой композиции выполняется совмещение векторов доминирующих цветов, каждый из которых представляет свою область. В методе построения иерархии кусочно-постоянных приближений, наоборот, кластерные алгоритмы работают по всему полю изображения, но на обрабатываемые множества накладываются ограничения, например, рассматриваются только смежные пары сегментов.

2. В методе сегментации по цвету и текстуре спорным моментом остается выбор параметров кластеризации в алгоритме адаптивной кластеризации, *K-means* и выбор ограниченного набора текстур. В то время как в методе построения кусочно-постоянных приближений сегментированного изображения параметр кластеризации отсутствует, а результатом алгоритма является множество приближений изображения.

3. Еще одним спорным моментом метода сегментации по цвету и текстуре является требование задания кодовой книги цветов (*color codebook*), значения которой служат индикаторами построения графа минимальной стоимости (*minimal cost graph*) в задаче вычисления оптимального расстояния цветовой композиции (OCCD) К тому же вычислительная сложность метрики OCCD близка к кубической, что снижает скорость вычислений.

4. В [1] недостаточно освещается вопрос о способе разбиения изображения на участки, для которых вычисляются доминирующие цвета при помощи алгоритма адаптивной кластеризации.

По всей видимости в развитии применения [1] определенный интерес представляет исследование возможностей алгоритма Команицу-Мейера. На выходе алгоритма – карта доминирующих цветов и соответствующее ей изображение, 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.

СПИСОК ЛИТЕРАТУРЫ

1. Chen, J., Pappas, T. N., Mojsilovic, A., & Rogowitz, B. (2002, June). Adaptive image segmentation based on color and texture. In *Image Processing. 2002. Proceedings. 2002 International Conference on* (Vol. 3, pp. 777–780). IEEE.
2. W.Y. Ma, Y.Deng, B.S. Manjunath, “Tools for texture/color based search of images,” *Human Vision and Electronic Imaging II*, Feb. 1997, Proc. SPIE, Vol. 3016, p. 496–507.
3. D. Comaniciu, P. Meer, “Robust analysis of feature spaces: Color image segmentation,” CVPR, June 1997, p. 750–755.
4. T.N. Pappas, “An adaptive clustering algorithm for image segmentation,” IEEE Tr. SP, v. 40, p. 901–914, Apr. 1992.
5. M.M. Chang, M.I. Sezan, A.M. Tekalp, “Adaptive Bayesian segmentation of color images,” JEI, p. 404–414, Oct. 1994.
6. A. Mojsilovic, J. Hu, E. Soljanin, “Extraction of perceptually important colors and similarity measurement for image matching, retrieval, and analysis,” IEEE Tr. IP.
7. A. Cohen, I. Daubechies, J. C. Feauveau, “Biorthogonal bases of compactly supported wavelets,” *Commun. Pure Appl. Math.*, v. 45, p. 485–560, 1992.
8. R. Chitta, M. Narasimha Murty, Two-level k-means clustering algorithm for k-τ relationship establishment and linear-time classification, Pattern Recogn. 43 (3) (2010), 796–804.
9. М.В. Харинов, И.Г. Ханыков, Оптимизация кусочно-постоянного приближения сегментированного изображения. Труды СПИИРАН. 3 (40). С. 183–202, 2015.
10. М.В. Харинов, И.Г. Ханыков, Комбинированный метод улучшения сегментации изображения. Вестник БГУ, С.118–124, 2015.
11. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Прикладная статистика: Классификация и снижение размерности. – М.: Финансы и статистика, 1989. – 607 с.
12. Харинов М.В. Альтернатива иерархическому методу Оцу для цветового изображения // Вестн. Бурят. гос. ун–та. 2014. – №9. – С. 64–72.
13. Mumford D., Shah J. Optimal Approximations by Piecewise Smooth Functions and Associated Variational Problems // Communications on Pure and Applied Mathematics. 1989. Vol. XLII, №4. pp. 577-685.
14. Бугаев А.С., Хельвас А.В. Поисковые исследования и разработка методов и средств анализа и автоматического распознавания потоковой информации в глобальных информационных системах. Шифр «Лацкан» // Отчет по НИР. – М.: Изд-во МФТИ, 2001. – Т. 1. – 140 с.
15. Crisp D.J., Tao T.C. Fast Region Merging Algorithms for Image Segmentation // The 5th Asian Conference on Computer Vision (ACCV2002). 23–25 January 2002. Melbourne, Australia. pp. 1–6.
16. Харинов М.В. Улучшение качества приближения цифрового изображения на основе иерархической сегментации // Вестн. Бурят. гос. Ун-та. 2014. – №9 (3). – С. 54-57.
17. Ward J.H., Jr. Hierarchical grouping to optimize an objective function. // J. Am. Stat. Assoc. 1963. Vol. 58, Issue 301, pp. 236-244.
18. M.V. Kharinov Model of the quasi-optimal hierarchical segmentation of a color image // Journal of Optical Technology. Vol. 82, Issue 7, pp. 425–429, (2015).
19. M.V. Kharinov Pixel Clustering for Color Image Segmentation // Programming and Computer Software, 2015, Vol. 41, No5, pp. 258–266. © Pleiades Publishing, Ltd., 2015.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

ПРОБЛЕМЫ, ЦЕЛИ И ЗАДАЧИ УНИФИКАЦИИ КЛЮЧЕВЫХ СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Устинов Игорь Анатольевич,
ОАО «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Обручевых, д.1,
e-mail: npoimpuls@peterlink.ru.

Аннотация: В статье рассмотрены ключевые системы информационных инфраструктур, их структура, классы, разработка.

Ключевые слова*: критические инфраструктуры; критическая информационная технология; ключевых систем информационных инфраструктур; ключевые (критические) информационно-управляющие системы*

CHALLENGES, GOALS AND OBJECTIVES OF THE UNIFICATION OF KEY MANAGEMENT SYSTEMS CRITICAL INFRASTRUCTURE

Ustinov Igor,
«Scientific-Production Association «Impulse»,
Russia, St. Petersburg, ul. Obrucheva, 1,
e-mail: npoimpuls@peterlink.ru.

Abstract: This paper examines the key system information infrastructures, their structure, classes, working out.

Keywords: *critical infrastructure; critical information technology; key systems of information infrastructures; key (critical) information management systems*

Введение

Критические инфраструктуры играют жизнеопределяющую роль в деятельности страны. Выход из строя или уничтожение объектов и средств критических инфраструктур (обороны, транспорта, энергетики и т.д.) может привести к губительным, неприемлемым последствиям для страны.

Ведущая роль в обеспечении необходимого качества функционирования критических инфраструктур принадлежит совокупности методов, аппаратно-программных и производственных средств, объединенных в единую критическую информационную технологию (КИТ), обеспечивающую разработку и сопровождение объектов критической инфраструктуры.

Основную роль в КИТ играют ключевые (критические) информационно-управляющие системы, которые управляют жизненно важными объектами или процессами критической инфраструктуры. К таким системам предъявляются особые, повышенные требования по надежности, живучести, безопасности, вероятностно-временным характеристикам и др.

При всем разнообразии критических инфраструктур можно выделить показатели их функционирования общие для всех инфраструктур, определяющие соответствующую инфраструктуру как критическую, жизненно необходимую стране, требующую особые меры по обеспечению надежного функционирования ее ключевых объектов и средств их информационных технологий.

Большое разнообразие критических инфраструктур потенциально ведет к многообразию ключевых систем информационных инфраструктур (КСИИ). Создание КСИИ требует значительных финансовых и материальных затрат. Разработка КСИИ для всех информационных инфраструктур усугубляет эту проблему, поэтому возникает насущная актуальная проблема унификации КСИИ для всего пространства ИИ.

Цель работы состоит в том, чтобы упорядочить разнообразие КСИИ. Определить границы унификации КСИИ с целью формирования концепцииразвития всех КСИИ как единого информационного пространства критических инфраструктур. Поэтому, в задачи работы входит определение научно-технических решений унифицированных КСИИ, обеспечивающих перспективу развития КСИИ.

Методической основой для решения данной проблемы является общность требований к качеству ИИ всех КИ. (Принцип единства требований)

Требования, предъявляемые к информационным технологиям в критических инфраструктурах можно разделить на две группы:

1. Общие требования для всех информационных технологий вкритических инфраструктурах, определяющие условияфункционирования ключевых систем управления ключевымиобъектами критических инфраструктур независимо от типаинфраструктуры;

2. Частные требования для каждой инфраструктуры, определяющиеиндивидуальные особенности ключевых объектов соответствующейинфраструктуры.

К показателям, образующим общую группу требований ко всем информационным технологиям независимо от их типа, относятся требования по надежности, живучести, информационной безопасности, вероятностно-временным характеристикам, технико-экономическим показателям и др. Требования по указанным показателям являются особо жесткими для всех информационных технологий в критических инфраструктурах независимо от того, является ли ключевым объектом космическая ракета, атомнаяэлектростанция, железнодорожный поезд или объект другой инфраструктуры, предъявляющий повышенныетребования к качеству функционирования.

Реализация общих требований ведет к возможности создания единых, унифицированных системотехнических решений для ключевых систем по архитектуре систем, телекоммуникациям, вычислительным средствам, защите информации, программному и информационному обеспечению и т.д.

Указанные общие требования дополняются для каждой ключевой системы частными требованиями, отражающими особенности управления и функционирования объектов соответствующей критической инфраструктуры.

Таким образом, можно представить новый взгляд на множество информационных технологий в критических инфраструктурах как единое информационное пространство с унифицированными средствами управления ключевыми объектами этого пространства.

В зависимости от уровня решаемых задач, объема предъявленных требований унифицированные КСИИ (УКСИИ) можно разделить на следующие классы:

1) Командные системы управления (КСУ);
2) Информационно-управляющие системы (ИУС);
3) Информационные системы (ИС).

Требования к УКСИИ определяются ее классом.

В общем виде УКСИИ есть совокупность звеньев управления (ЗУ) объединенных каналами связи различной физической природы в единую сеть, которая работает на основе сетевых протоколов. УКСИИ взаимодействует с ключевыми объектами через ЗУ посредством оконечного оборудования данных звена.

Система, выполненная на единой, унифицированной, масштабируемойвычислительно-коммутационный платформе, соответствует требованиям, предъявляемым к различным видам базирования и уровням управления.

Унификация аппаратно-программных средств, построенных на современной стойкой ЭКБ, позволяет существенно повысить эксплуатационные характеристики аппаратных и программных средств, технологичность отладки и проверки,и в целом, качество изготовления и сопровождения аппаратуры в течение всего жизненного цикла.

Средой передачи данных и основой информационной структуры аппаратной платформы является структура ЛВС на базе технологии Ethernet10Base-T. оснащенная дублированными каналами сети и выполненная с высоким уровнем резервирования аппаратных вычислительных средств.

В общем случае звено УКСИИ состоит из двух секторов:

– унифицированного сектора (СУ);
– индивидуального сектора (СИ).

СУ отражает общие свойства КИ.

СИ определяет особенности конкретной КИ.

СУ обеспечивает передачу и обработку информации на всех объектах системы на основе единых протоколов информационного обеспечения, единой логики взаимодействия и форматов кодограмм по специальным каналам.

В состав СУ, выполненного на базе унифицированных масштабируемых модулей, входят интегрированные средства обмена данными, образующие тракты передачи системы.

Схемотехнически составные части платформы представляют собой набор функционально законченных приборов, электрически связанных между собой в требуемой комбинации. При этом прибор является типовым элементом замены, что повышает надёжность электрических соединений за счёт снижения количества сочленений-расчленений внутренних разъёмов прибора («модуль-прибор») в процессе его настройки и эксплуатации.

Аппаратная платформа реализована ограниченной номенклатурой приборов и модулей.

Научно-технические результаты, полученные в НПО «Импульс», обеспечивают выполнение самых высоких требований к системам:

– непрерывность функционирования в течение многих лет без прерывания управления;

– функционирование с накоплением неисправностей, в том числе на необслуживаемых объектах в течение межрегламентного режима;

– защищенность от воздействия максимально широкого спектра различных воздействий на систему и аппаратуру различного базирования;

– высокий уровень информационной защищенности систем;

– технологическую безопасность за счет применения отечественной элементной базы;

– способность развиваться в сложных условиях эксплуатации;

– высокие эксплуатационные характеристики.

Эти показатели обеспечены путем применения разработанного комплекса технологических мер по обеспечению высокой надежности и устойчивости создаваемой аппаратуры к различным воздействиям. В состав этих мер, в частности, входят:

– обоснованный выбор базового логического элемента с освоениемсерийного производства на отечественных заводах;

– разработка оптимальных схемно-конструкторских решений аппаратуры;

– выбор широкой области устойчивости работы схем;

– использование различных видов избыточности (функциональной, структурной и тр.) на различных уровнях систем, резервирование (дублирование) отдельных элементов и узлов;

– разработка комплекса мер по обеспечению стойкости создаваемой аппаратуры к различным воздействиям (электромагнитных полей, грозовыхразрядов, ионизирующих воздействий естественного и искусственного происхождения и т.д.);

– разработка комплекса мер защиты от различных воздействий на информациюи аппаратуру;

– тщательная отработка документации на опытных образцах;

– тщательная отработка программного обеспечения изделий на инструментальных и комплексных стендах;

– всесторонние испытания разработанных изделий.

Состав звеньев, разработанных по указанной технологии, может быть положен в основу создания единого ряда звеньев УКСИИ.

Заключение

Работы по унифицированному сектору звена могут составлять значительную долю всех работ по звену (в зависимости от ранга звена), поэтому реализация предлагаемой унификации ключевых систем даст, учитывая масштабы информационной инфраструктуры, значительный экономический эффект на всех жизненных этапах УКСИИ.

Разработано и успешно функционирует более 20 АСУ и ИУС, созданных по изложенной технологии и техническим решениям [1, 2].

СПИСОК ЛИТЕРАТУРЫ

1. Устинов И.А., Игумнов В.В. Информационные технологии в критических инфраструктурах. XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2010)»: Труды конференции. Секция: Информационные технологии в критических инфраструктурах. – СПб, 2010
2. Устинов И.А., Игумнов В.В. Информационная безопасность в критических инфраструктурах. VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011)»: Труды конференции. Секция: Информационная безопасность в критических инфраструктурах – СПб, 2011
3. Устинов И.А., Журавлева О.П. «Новые технологии работы с информацией OL «IMPULS». XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2010)»: Труды конференции. Секция: Информационные технологии в критических инфраструктурах. - СПб, 2010.
4. Устинов И.А., Петухов В.Е., Игумнов В.В., Александров А.М. О концепции «Информационные технологии в критических инфраструктурах» XII Санкт-Петербургская международная конференция «Региональная информатика (РК-2012)»: Труды конференции. Секция: Информационные технологии в критических инфраструктурах. - СПб, 2012.

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Устинов Игорь Анатольевич, Игумнов Владимир Вячеславович,
ОАО «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Обручевых, д.1,
e-mail: npoimpuls@peterlink.ru.

Аннотация: В статье рассмотрены требования к проектируемым системам на основании технологии создания защищенных ключевых информационно-управляющих систем.

***Ключевые слова**: ключевые информационно-управляющие системы критических инфраструкту; информационно-управляющие системы; командные системы управления.*

INFORMATION MANAGEMENT SYSTEM TO ENSURE INFORMATION SECURITY IN CRITICAL INFRASTRUCTURES

Ustinov Igor, Igumnov Vladimir,
"Scientific-Production Association «Impulse»,
Russia, St. Petersburg, ul. Obrucheva, 1,
e-mail: npoimpuls@peterlink.ru.

Abstract: The article deals with the requirements for the designed system based on the technology of secure key management information systems.

***Key words**: information-control systems of critical infrastruc; management information systems; command control system.*

Введение

Информационная безопасность это комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей автоматизированной информационной системы. Иными словами, это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Отдельные сферы деятельности систем государственного, военного, финансового управлений, информационные и телекоммуникационные системы, объекты экономики, транспорта, энергетики и т. д. (так называемые критические инфраструктуры) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых задач. Критические инфраструктуры это системы объектов, услуг и информационные системы для которых неисправность или уничтожение отдельных элементов будут иметь серьезные негативные последствия для здоровья и безопасности населения, окружающей среды, национальной экономики, обороны и т.д.

Информационная безопасность относится к числу важнейших характеристик критических инфраструктур. Это относится как к информационной безопасности в целом, так и к безопасности информации в частности. При этом ведущая роль в обеспечении информационной безопасности принадлежит ключевой информационно-управляющей системе данной критической инфраструктуры.

Решение этой фундаментальной проблемы и ее контроль проходит на всех этапах жизненного цикла создания информационно-управляющих систем для критических инфраструктур - от проектирования, изготовления, испытаний, эксплуатации и до утилизации. Меры, принимаемые для ее решения, должны быть адекватны для нейтрализации возможного ущерба от деструктивных воздействий на ключевые инфраструктуры.

Технические требования к ключевым информационно-управляющим системам критических инфраструктур определяются классом решаемых ими задач и задаются соответствующими тактико-техническими заданиями Государственных Заказчиков. Отсюда определяются основные требования к алгоритмам функционирования системы, требования к выбору и применению электронной компонентной базы, схемно-конструкторским решениям, программному обеспечению, системе защиты процессов и процедур обработки информации и защиты самих объектов системы, к защите каналов связи, подавлению побочных электромагнитных излучений, алгоритмам диагностики и контроля комплексов средств автоматизации, технологии отработки и проведения всего комплекса испытаний с максимальным подтверждением заданных требований в условиях стендовой базы предприятия и т. д.

В ОАО «НПО «Импульс» сформирована особая отечественная научно-техническая школа в области создания больших информационных систем. Научные рекомендации этой школы определили технологию создания защищенных (оборона, атомная энергетика и др.) ключевых информационно-управляющих систем. Полученные на этой технологии решения позволяют выполнить основные требования к проектируемым системам. Это – высокая надежность систем, сохранение работоспособности систем при частичных отказах, гарантированная защита информации от различных воздействий, уникальные вероятностно-временные характеристики передачи данных, способность к развитию, высокие эксплуатационные характеристики. Правильность данной технологии подтверждена на практике разработкой и успешным функционированием более 20 созданных автоматизированных систем управления и информационно-управляющих территориально-распределенных систем, обеспечивающих надежное управление объектами различных Заказчиков от Министерства Обороны РФ, Роскосмоса, Росатома.

Ключевые системы для критических инфраструктур (автоматизированные системы управления специального назначения) в зависимости от уровня решаемых задач условно можно разделить на два основных класса – информационно-управляющие системы и командные системы управления.

Функциональные требования и условия применения этих двух классов систем существенно отличаются друг от друга, что неизбежно отражается на технической политике по созданию систем и по обеспечению их информационной безопасности. Не последняя роль здесь принадлежит правильному выбору электронной компонентной базы.

Информационно-управляющие системы чаще всего построены в основном на применении импортных аппаратных, программных и технологических решениях и, обеспечивают функционирование в мирное время и в начальный период ухудшения военно-политической обстановки.

Командные системы управления требуют высокого уровня технологической независимости и информационной безопасности и должны обеспечивать функции управления объектами, в том числе и необслуживаемыми, с высокой вероятностью выполнения поставленных Руководством страны задач во всех условиях функционирования государства.

В связи с этим должны предъявляться особые требования к «кирпичикам» построения ключевых защищенных систем – элементной базе, она должна быть сугубо отечественная и российского производства.

Применение импортной элементной базы и импортного программного обеспечения не гарантирует необходимый уровень информационной защиты из-за возможного наличия в ней различных «закладок». Наличие этих вредоносных вставок, может привести к блокированию выполнения системой основных функций, в случае перевода ее в режим применения, неприемлемый для эвентуального противника, и соответственно делает данную ключевую информационно-управляющую систему критической инфраструктуры беззащитной в конфликтных ситуациях.

Гарантированное противостояние угрозам и обеспечение требуемого уровня информационной безопасности возможно надежно обеспечить применением доверительных отечественных программно-аппаратных платформ при создании систем, ее составных частей и комплексов средств автоматизации. Проблемам обеспечения кибер-безопасности в информационных системах и создания доверительных отечественных программно-аппаратных платформ были посвящены в этом году ряд совещаний в Руководстве страны, что подчеркивает их важность и актуальность на современном этапе.

Свойство доверительности означает однозначное соответствие работы ключевой информационно-управляющей системы критической инфраструктуры алгоритмам и функциям, заложенным в неё для выполнения основной задачи. Доверительность означает также предсказуемость поведения этой системы в соответствии с тактико-техническими требованиями на всём наборе внешних воздействующих факторов. Свойство доверительности должно обеспечиваться как в самих защищенных ключевых системах, так и в технологиях их создания, исключающих утечку проектной информации, минимизацию инженерных ошибок и исключающих внедрение недекларированных возможностей в конечный продукт.

Понятие доверительности сложилось в ОАО «НПО «Импульс» в процессе создания автоматизированных систем управления специального назначения критических инфраструктур на протяжении более 50-летней напряженной инженерной деятельности объединения. Доверительность не является новым свойством для систем разработки нашего объединения, так как они (системы) проектируются на отечественной радиационно-стойкой электронной компонентной базе и на программном обеспечении собственной разработки, на базе доверительных операционных систем.

Необходимо отметить, что постоянно растущая сложность и объемы задач управления требует интенсивного развития отечественной электронной компонентной базы, ее максимального быстродействия, максимальных объемов памяти, сверхмалых габаритов и энергопотребления.

Общие тенденции развития автоматизированных систем управления специального назначения определяют сближение функций информационно-управляющих и командных систем заставляя искать разработчиков варианты их технической реализации. ОАО «НПО «Импульс» принципиально решило эту задачу, предлагая в единой системе реализацию независимых функциональных элементов в общем конструктиве на базе отечественной электронной компонентной базы.

Сегодня особенностями создания автоматизированных систем управления специального назначения критических инфраструктур для Министерства Обороны РФ являются их функционирование (в ближайшей перспективе) в рамках единого информационно-коммуникационного пространства. Концепция единого информационно-коммуникационного пространства предполагает создание единой глобальной информационной среды, обеспечивающей комплексную обработку сведений в масштабе времени, близком к реальному, об эвентуальном противнике, о возможностях своих структурных подразделений и окружающей местности в интересах обеспечения принятия решений по вопросам оптимального и эффективного управления в различной обстановке.

Решение задачи интеграции создаваемых систем в единое информационно-коммуникационное пространство лежит в плоскости комплексного внедрения новейших цифровых технологий при формировании интегрированных информационно-вычислительных сетей различного масштаба. Поэтому новое поколение автоматизированных систем управления специального назначения в интересах Министерства Обороны РФ должно быть построено по сетевому принципу и иметь многоуровневую иерархическую структуру. Это позволит организовать информационное сопряжение с аналогичными системами других критических инфраструктур.

Основой для технологической архитектуры перспективных автоматизированных систем управления специального назначения является «принцип открытой системы», который состоит в создании среды, включающей программные и аппаратные средства, службы связи, интерфейсы, форматы данных и протоколы, которая в своей основе имеет развивающиеся, доступные и общепризнанные стандарты и обеспечивает масштабируемость системы, переносимость и взаимодействие приложений и данных. При этом информационная защищенность системы остается приоритетным направлением работ и одним из основных критериев оценки её работоспособности.

Заключение

ОАО «НПО «Импульс» проводит в настоящее время комплекс опытно-конструкторских работ по созданию таких современных автоматизированных систем управления специального назначения «под ключ». Разработанные новые базовые несущие конструкции (модуль, прибор, шкаф монтажный), программно-аппаратные платформы сугубо на отечественной электронной компонентной базе российского производства, позволяющие создавать отказоустойчивые информационно-вычислительный комплексы, комплексы средств передачи данных, в том числе для перспективных цифровых каналов, доверительная программная среда, уникальные унифицированные алгоритмы управления и специальные технические решения и средства в обеспечение высокого уровня информационной безопасности позволяют создавать информационно-управляющие системы и их составные компоненты практически для любой критической инфраструктуры с комплексным решением вопросов по информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности РФ. Утверждена Президентом РФ 9.09.2000. Пр-1895.
2. Закон РФ «О безопасности» (с изм. 02.03.2007). Утв. Президентом 05.03.1992. № 2446-I.
3. Стратегия национальной безопасности России до 2020 г. Утверждена указом Президента №357 от 12.05.2009.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

УДК 004.5 / 13.00.08

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ: СЕМИОТИЧЕСКИЙ ПОДХОД

Государев Илья Борисович,
Российский государственный педагогический университет им. А.И. Герцена,
Россия, Санкт-Петербург, наб. р. Мойки, д. 48,
e-mail: gossoudarev@herzen.spb.ru

***Аннотация**:* В статье рассмотрен подход к электронному обучению (e-learning) и технологиям электронного образования с позиций знаковых систем, включающий изучение формальных языков как пререквизит деятельности по разработке ЭОР.

***Ключевые слова**: электронное образование; формальные языки, семиотика, веб-технологии; веб-разработка.*

E-LEARNING TECHNOLOGIES: SEMIOTIC APPROACH

Ilya Borisovich Gosudarev,
The Herzen State Pedagogical University of Russia,
Russia, St. Petersburg, nab. r. Moiki 48,
e-mail: gossoudarev@herzen.spb.ru

Abstract: The article describes an approach towards e-learning from the point of view of formal systems, including studying formal languages as a prerequisite for web developing.

***Keywords**: e-learning; formal languages, semiotics, web technology; web development*

Введение. Термин «электронное образование», относительно редко встречающийся в литературе по сравнению с термином «электронное обучение», понимается нами как расширение последнего, долженствующее охватить решение всего спектра образовательных задач с помощью адекватных информационных и коммуникационных технологий. При этом *обучение* с помощью ИКТ в терминологии ЮНЕСКО и в соответствии с национальным стандартом РФ ГОСТ Р 52653-2006 называется электронным обучением (e-learning). Отметим, что закон об образовании РФ в редакции от 28.02.2012 включил в себя обновленную версию этой трактовки: «организация образовательного процесса с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологии, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие участников образовательного процесса». Ключевыми в двух определениях являются схемы их построения: *«обучение»* | *«организация образовательного процесса»* – *«с помощью»* | *«с применением».*

В статье [4] К.Р. Пиотровская называет «семиотическим» подход, который, «рассматривая педагогические вопросы, ставит во главу угла увязку содержания, целей, средств и методов образования со структурой и функционированием различных знаковых систем». В своей кандидатской диссертации [1] автором данной статьи была предложена модель разработки профильных (или, в современной терминологии, *элективных*) курсов по информатике, основанная на сопоставлении содержанию курсов некоторых языков разметки. Например, языковой основой теоретических курсов в области «математических основ информатики» или прикладных курсов в области «математического программного обеспечения» предлагалось считать язык разметки математических текстов MathML. В настоящее время, с учетом диверсификации технологий и необходимости выделения некоторого ясно различимого принципа их отбора адекватно решаемым образовательным задачам, эта концепция вновь представляется потенциально плодотворной.

Мы приходим к этому, исходя из следующих предпосылок. Во-первых, рассмотрение символьных, знаковых систем и формальных языков является задачей педагогической деятельности автора данной статьи в процессе взаимодействия со студентами бакалавриата «Информатика и

вычислительная техника» на факультете информационных технологий РГПУ им. А.И. Герцена. Во-вторых, к необходимости обращения к формальным языкам (формальным системам) как основе технологий электронного обучения и образования приводит задача экспликации самих по себе терминов «электронное обучение» и «электронное образование» и тесно связанного с ними термина «(электронная) информационно-образовательная среда» (ЭИОС).

Данный термин отличается многообразием трактовок и определений разного типа. Например, в [3] автор предлагает использовать следующее определение: «информационно-образовательная среда вуза – педагогическая система, объединяющая в себе информационные образовательные ресурсы, компьютерные средства обучения, средства управления образовательным процессом, педагогические приемы, методы и технологии, направленные на формирование интеллектуально развитой социально-значимой творческой личности, обладающей необходимым уровнем профессиональных знаний и компетенции». Понятие ИОС получило «официальное» определение в федеральных государственных стандартах начального и общего образования, а впоследствии в упомянутом выше федеральном законе об образовании РФ. В соответствии с ГОСТ Р 53620-2009, ИОС – это система инструментальных средств и ресурсов, обеспечивающих условия для реализации образовательной деятельности на основе информационно-коммуникационных технологий. ФГОС ООО определяет следующую конкретную структуру ИОС:

– комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы;

– совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное ИКТ оборудование, коммуникационные каналы;

– систему современных педагогических технологий, обеспечивающих обучение в современной ИОС.

Закон об образовании РФ включил в себя обновленную версию этой трактовки (ст.16, п.3): ЭИОС – это электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, обеспечивающие освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся. Отсюда можно заключить, сравнивая с определениями, приведенными в начале данной статьи, что в совокупной трактовке российских нормативных документов и других источников *электронным* следует считать *обучение в ЭИОС*. Отметим, что до появления «официальных» определений авторы Концепции ИОС открытого образования РФ С.Л. Лобачев, А.А. Поляков, В.И. Солдаткин предлагали следующее определение [2]: «Информационно-образовательная среда (ИОС) – программно-телекоммуникационное и педагогическое пространство с едиными технологическими средствами ведения учебного процесса, его информационной поддержкой и документированием в среде Интернет любому числу учебных заведений, независимо от их профессиональной специализации (уровня предлагаемого образования), организационно-правовой формы и формы собственности».

Приведенные выше типичные примеры определений ЭИОС характеризуются глобальностью (речь идет о средах «вообще»), статичностью (фиксируется начальное состояние или условия без описания динамических характеристик) и определенной противоречивостью – они все включают нерядоположенные элементы, относящиеся к совершенно разным смысловым рядам, например, «телекоммуникации» и «педагогические технологии», «базы данных» и «педагогическое пространство». С другой стороны, сам по себе термин «электронное обучение» является ничем иным, как не вполне корректной калькой англоязычного термина «e-learning», в дословном переводе «электронное учение». В связи с этим представляется целесообразным осуществить следующее:

1. Дать системное конструктивное определение для ЭИОС, имеющее процессуальный характер, предполагающее возможность развития;

2. Определить термин «электронное обучение» и термин «электронное образование» как систему деятельностей, направленных на решение образовательных задач и осуществляемых в ЭИОС.

Итак, будем говорить, что задана (определена, развернута) ЭИОС учебного модуля (компонента содержания образовательной программы), если определен кортеж <E, P, L>:

– содержание модуля M (образовательной программы) доступно в виде электронных образовательных ресурсов (ЭОР);

– развернута программная система P (платформа) типа системы дистанционного обучения (LMS) с возможностью импорта этих ЭОР или доступна система программных решений с такой же совокупной функциональностью, позволяющих организовать взаимодействие потребителя с ЭОР;

– выбран некоторый язык L или совокупность языков, обеспечивающих коммуникацию внутри указанной системы и наполняемость ее результатами образовательной деятельности.

Под «наполняемостью» результатами образовательной деятельности понимается возможность развития, динамического «достраивания» ЭИОС субъектами взаимодействий, например, путем размещения электронных портфолио лиц, осуществляющих взаимодействия. Тем самым задается

возможность эволюции этой структуры во времени. Данное рабочее определение предъявляет конструктивные требования к организационным условиям образовательной деятельности, носит системный характер и является масштабируемым, то есть применимым к разным уровням организации образовательной деятельности.

Под языками, обеспечивающими коммуникацию внутри системы и наполнение ее результатами учебной деятельности понимаются как естественные языки (метаязыки исследователя систем, такие как «обычный» русский или английский язык) с выделенной и разделяемой всеми субъектами терминологией («ЭОР», «интерфейс», «URL-адрес», «браузер», «SCORM-пакет» и так далее), так и искусственные (формальные) языки, используемые для создания учебного контента.

В качестве примеров очевидного и получающего все большее распространение подобного формального языка приведем регулярный язык адресов URL и контекстно-свободный язык HTML5 (язык разметки гипертекста пятой версии, актуальной на момент написания данной статьи). Общие представления о синтаксисе HTML и представления об отдельных его командах (так называемых тегах) оказываются совершенно необходимыми для решения простейших задач, связанных с модификацией образовательного контента.

Например, при возникновении необходимости разместить гипертекстовую ссылку, *любой* пользователь ЭИОС должен отличать относительные ссылки от абсолютных по признаку наличия протокола вида http:// в начале URL-адреса, а также различать повторяемость шаблонных фрагментов внутри URL. Размещение самой по себе гиперссылки очень часто связано с редактированием тега Такого рода знания вышли за пределы предметных результатов обучения информатике в основной школе и стали метапредметными.

В случае с будущими инженерами, конечно, диапазон используемых языков драматически возрастает и связан он, в первую очередь, с вебом. Это главным образом языки клиентской стороны CSS, XML, SVG, RSS, Javascript. Причем язык Javascript с распространением серверной технологии Node.js / IO.js начинает играть роль универсального кроссплатформенного клиент-серверного языка сценариев и программирования. Более того, характерные особенности и идиомы Javascript позволяют использовать его в качестве метаязыка для описания тех или иных ситуаций программирования на других языках (до сих пор в этой роли часто фигурировал Pascal).

Так называемые фреймворки или библиотеки, наподобие jQuery, Ember или AngularJS, играют роль языков-надстроек над «родительским языком», заменяя исходные идиомы новыми, более прозрачными, лаконичными и доступными для понимания даже начинающими разработчиками.

До недавнего времени существовало достаточно четкое разделение уровней работы с платформами: уровень конечных пользователей и уровень разработчиков. Для современного этапа характерно размывание этих различий. Конечные пользователи платформ принимают участие в разработке ресурсов (например, вики), используют теги языков разметки для вставки мультимедийных компонент и фрагментарно задействуют элементы программирования на таких языках как Javascript. Разработка мультимедийных интерактивных ресурсов перемещается в веб. Причем если на данном этапе в вебе располагаются, прежде всего, платформы (а ресурсы для них частично изготавливаются с помощью десктоп-приложений, таких как видеоредакторы), то с развитием онлайн-редакторов и облачных хранилищ перспективным представляется перемещение *всей* деятельности по разработке ЭОР любой сложности в веб.

В настоящее время все большее распространение приобретают так называемые облачные хостинги (Selectel, Cloud4Y, DigitalOcean и др.), предоставляющие платформу как регулируемую услугу. В других статьях автором описан опыт развертывания инновационной учебной среды edX на платформе DigitalOcean в интеграции с Moodle и инструментами бордкастинга, такими как Кодактор (kodaktor.ru или dist-learn.spb.ru). Такие решения превращают ЭИОС в мобильную среду (МЭИОС), характеризующуюся независимостью от географического расположения. С учетом этого опыта автором сформулирована концепция подготовки студентов (РГПУ им. А.И. Герцена) к деятельности в условиях современных МЭИОС на базе подобных платформ, основными положениями которой являются следующие:

1. Студенты и преподаватели являются одновременно корпоративными пользователями и соразработчиками МЭИОС, создавая ресурсы в ее рамках.

2. В основе работы с платформами на разных уровнях лежат те или иные формальные языки, в первую очередь HTML.

3. Одновременность и коллаборативность взаимодействия подразумевает лишь относительное опережение преподавателями студентов в аспекте освоения новых технологий и обуславливает превалирующую роль преподавателей как консультантов, фацилитаторов и соразработчиков; роль интеграторов взаимодействий играют выбранные языки и вся МЭИОС в целом.

4. Осваиваемое содержание часто носит аутсорсинговый характер и привязывается к платформе в виде ссылок на массовые открытые онлайновые курсы (МООК) других платформ (таких как Coursera или Lektorium.tv).

5. Глубина освоения инструментов разработки, а также выбор языковых средств (языков разметки) зависит от начального уровня и профиля (направления) подготовки студентов.

6. Среда взаимодействия (и разработки) едина для всех пользователей, но отдельные ее компоненты используются только студентами инженерных направлений. (Например, полнодуплексное клиент-серверное взаимодействие обеспечивается с помощью Node.js в пределах всей платформы, однако программирование для Node.js изучается только в рамках курса «Веб-проектирование» для будущих инженеров).

7. Мобильность МЭИОС определяется возможностью доступа к платформе через веб, а также независимостью от месторасположения пользователей и от установленного на их клиентских устройствах программного обеспечения.

Заключение. Нами предложен подход к электронному обучению (e-learning) и технологиям электронного образования с позиций знаковых (формальных) систем, включающий изучение формальных языков как пререквизит деятельности по разработке ЭОР, рассматривающий ЭИОС как систему в развитии, основанную на формальных языках и адекватно выбранных платформах.

СПИСОК ЛИТЕРАТУРЫ

1. Государев И.Б. Подготовка будущих учителей информатики к проектированию профильных курсов веб-технологий: автореферат дисс. к.п.н. – СПб., 2004.
2. Лобачев С.Л., Поляков А.А. Универсальная инструментальная информационно-образовательная среда системы открытого образования Российской Федерации. Лекция-доклад // Третья Всероссийская Школа-семинар «Информационные технологии в управлении качеством образования и развитии образовательного пространства». – М.: Исследовательский центр проблем качества подготовки специалистов, 2001, 40с.
3. Остроумова Е.Н. Информационно-образовательная среда вуза как фактор профессионально-личностного саморазвития будущего специалиста // Фундаментальные исследования. – 2011, №4, С.37–40, [Электронный ресурс] URL: www.rae.ru/fs/?section=content&op=show_article&article_id=7793628 (дата обращения: 23.05.2013).
4. Пиотровская К.Р. Базовые принципы построения методической теории обучения студентов-филологов математике и информатике // Известия РГПУ им. А.И. Герцена, 2005, №12, [Электронный ресурс] URL: http://cyberleninka.ru/article/n/bazovye-printsipy-postroeniya-metodicheskoy-teorii-obucheniya-studentov-filologov-matematike-i-informatike (дата обращения: 27.02.2015).

УДК 004.9, 378.14

ОБЗОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ В УЧЕБНОМ ПРОЦЕССЕ КАФЕДРЫ УНИВЕРСИТЕТА

Дмитриева Анастасия Валерьевна, Ключарев Александр Анатольевич,
Степанов Александр Георгиевич,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д.67,
e-mails: naglaya_90@list.ru, ak@aanet.ru, georgich_spb@mail.ru

Аннотация: Рассматриваются информационные системы, предназначенные для учебной, методической и организационной деятельностей кафедры в электронно-образовательную среде высшего учебного заведения созданной на основе системы управления обучением.

Ключевые слова: *система управления обучением; дистанционное обучение; moodle, синхронное обучение, асинхронное обучение.*

REVIEW OF INFORMATION TECHNOLOGY USED IN EDUCATIONAL PROCESS DEPARTMENTS OF THE UNIVERSITY

Anastasia Dmitrieva, Aleksandr Klucharev, Aleksandr Stepanov,
The St. Petersburg State University of aerospace instrumentation,
Russia, St. Petersburg, Bolshaya Morskaia str. 67,
e-mails: naglaya_90@list.ru, ak@aanet.ru, georgich_spb@mail.ru

Abstract: We consider the existing information systems for educational, methodical and organizational activities of the department in the electron-education among the educational institutions set up by the learning management system.

Keywords: *leaning management system; distance-based education; moodle; e-learning; synchronous distance education; asynchronous distance education.*

Введение. Традиционно кафедра является основным структурным подразделением университета, осуществляющим учебно-воспитательную, научно-исследовательскую, организационно-методическую и социальную деятельности. Кафедра может вести несколько направлений подготовки студентов и подготовки и переподготовки педагогических и научных кадров, а также выполнять научно-исследовательские работы. На кафедру возлагаются обязанности по

привлечению абитуриентов, проведению воспитательной работы со студентами, связи с выпускниками и учет их индивидуальных достижений. Кроме этого, кафедра решает большое количество организационно-управленческих задач, которые обеспечивают ее работу (распределение нагрузки, составление индивидуальных планов преподавателей, составление расписаний, ведение протоколов заседаний и т.п.). Учитывая относительно небольшую численность кадрового состава, в повседневной деятельности кафедры дополнительно встает задача организации внутренних коммуникаций между сотрудниками [1].

Существуя в условиях уже почти пятнадцатилетнего реформирования, высшая школа России, а вместе с ней и кафедры вузов, сталкиваются с очевидными трудностями. Среди них выделим проблемы, связанные с основными трудовыми ресурсами высшей школы – ее преподавателями [2]. Внедрение в практику «эффективного контракта» продолжает уже ставшую привычной для Министерства образования и науки интенсификацию труда работников высшей школы традиционными средствами [3], [4]. Анализируя сложившуюся ситуацию можно предположить, что существовавшие ранее возможности повышения производительности труда преподавателей, связанные с увеличением количества аудиторных часов, тарификацией видов занятий, уже исчерпаны [5], [6].

Альтернативу интенсификации составляет массовое внедрение информационных технологий в работу кафедр [7]. Их использование для обеспечения учебной, методической и организационной работы является уже требованием времени, а не просто модным приемом. Утвержденный 30 октября 2014 года новый федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)» требует от вузов наличия электронно-образовательной среды, аудиторий, оборудованных для визуального представления учебной информации, свободного доступа обучающихся к сети «Интернет» и к электронно-библиотечным системам, формирования электронного портфолио обучающегося, в том числе сохранение работ студентов, рецензий и оценок на эти работы со стороны любых участников образовательного процесса. Как отмечает Г.А. Григоров [8], «перед образованием стоят новые сложные задачи: подготовить личность к жизни в информационном обществе; сформировать у нее привычки продуктивной деятельности в условиях нового информационного образовательного пространства. Очевидно, для решения обозначенных задач необходимо кардинально изменить процесс образования, преодолеть массовое использование репродуктивного подхода в обучении и перейти к деятельностному обучению». Современная педагогика решает подобные задачи начиная со средней школы [9], а важнейшим инструментом, обеспечивающим требуемый результат, являются информационные технологии автоматизированного обучения [10].

Основным инструментом, формирующим электронно-образовательную среду, является автоматизированная информационная система, ориентированная на организацию и обеспечение учебного процесса. Существует несколько стандартов построения таких систем, среди которых упомянем SCORM – Sharable Content Object Reference Model (модель обмена учебными материалами). Этот стандарт является наиболее полным и распространенным мировым стандартом на электронные учебные материалы, который поддерживается большинством ведущих мировых производителей систем дистанционного обучения [11]. Среди собственно систем управления обучением упомянем LAMS, Sakai, ATutor, Claroline, Dokeos, OLAT, OpenACS, ILIAS. Большинство этих названий является аббревиатурами (например, London Academy of Management Sciences, Online Learning and Assessment Tool, Open Architecture Community System и т.п.). Судя по количеству публикаций на русском языке, в России (и Украине) наибольшее распространение получила система Moodle (Modular Object-Oriented Dynamic Learning Environment). Краткие характеристики перечисленных выше систем можно найти, например, в [12]. Несмотря на некоторые отличия интерфейсов систем управления обучением и наборов реализуемых функций, их возможности для основных пользователей – студентов, преподавателей и администрации высших учебных заведений – практически одинаковы: обеспечивать студента необходимым учебным материалом, дать возможность постоянного контакта студента с преподавателем, обеспечить свободный доступ к имеющимся на кафедре методическим материалам, контролировать ход учебного процесса; получать оперативную информацию об успеваемости.

Учебная работа кафедры предусматривает чтение лекций, проведение семинаров, практических занятий и лабораторных работ, курсовое проектирование, практики, организацию самостоятельной работы студентов, промежуточную и итоговую государственную аттестации, а также подготовку преподавателей к соответствующим видам занятий. Кроме этого, необходимо выполнять ряд операций, связанных с организацией учебного процесса (расчет и распределение нагрузки, разработка учебно-методических комплексов и т.п.).

Современные лекции предусматривают создание своих электронных вариантов [13]. Методика их разработки уже существует, базируется на программные пакеты типа Power Point или их аналоги, известна, достаточно распространена, а сами лекции пользуются популярностью у слушателей. Применение средств мультимедиа при преподавании специальных дисциплин уже становится вполне

привычным делом. О.В. Ощепкова [14] справедливо замечает, что они обеспечивают «совместно со слуховым и зрительный канал получения информации, наглядность не только способствует более успешному восприятию и запоминанию учебного материала, но и позволяет активизировать умственную деятельность, глубже проникнуть в суть изучаемых явлений, подтверждает регулирующую роль образа в деятельности человека». В литературе описаны особенности подготовки презентаций лекций с использованием презентаций по программированию [15], электротехнике [16], гуманитарным дисциплинам [17] и ряду других. Очень часто такие лекции называют лекциями – визуализациями. А.К. Томилин, развивая идеи визуализаций, отмечает, что «мультимедийные учебные материалы со звуковым сопровождением в наибольшей степени способны заменить реального преподавателя при самостоятельной работе студента», но при этом отмечает, что «лекционные видеокурсы не способны полностью заменить традиционные учебники и методические пособия [18].

Еще одной особенностью современной лекции является возможность участвовать в ней на расстоянии. Средства дистанционного общения типа Skype сейчас достаточно широко распространены. К сожалению, использовать их для проведения занятий неудобно из-за невозможности обслужить большое количество слушателей и передать одновременно с ней презентацию, рабочий стол компьютера или другую важную для понимания материала информацию. Известен набор профессиональных программных пакетов, позволяющих решить задачу дистанционного проведения учебных занятий. К ним относятся Adobe Acrobat Connect Pro, Elluminate, Dimdim, Open Meeting, Microsoft Office Live Meeting (на смену последней фирмой предлагается Lync).

Применительно к системе Microsoft Office Live Meeting аппаратная часть должна содержать Pentium – совместимый процессор с тактовой частотой 500 МГц и выше если Web-камера не используется. С использованием Web-камеры частота процессора должна быть 1 ГГц и выше. Кроме этого, требуется ОЗУ размером не менее 256 Мб (рекомендуется 512 Мб). Базовое программное обеспечение – операционная система Windows, начиная с XP Professional, а подключение к сети Интернет для передачи только звука и презентации – не менее 50 – 80 кбит/с, а при передаче дополнительно видеоизображения не менее 156 кбит/с [19]. Очевидно, что по современным меркам требования к аппаратуре и программному обеспечению не очень жесткие и доступны для подавляющего большинства пользователей.

При проведении семинарских и практических занятий информационные технологии обеспечивают возможность оперативной работы с учебной, справочной литературой, периодическими изданиями, программными и техническими средствами, позволяющими оперировать с разными выразительными средствами – текстом, графикой, звуком и видео [20].

Изначально лабораторные занятия предполагали физическое существование некого оборудования. Последнее время из соображений экономии реальные лабораторные стенды эмулировались программными средствами. Особое распространение такие лабораторные работы получили с развитием дистанционного обучения. Многие авторы, например, [21], [22], описывают программные реализации лабораторных работ на основе среды разработки лабораторных виртуальных приборов LabVIEW (Laboratory Virtual Instrument Engineering Workbench) созданной фирмой National Instruments (США) [23].

Основной формой формирования и контроля умений и навыков является курсовое проектирование по дисциплине, а также учебные практики. Главная проблема при организации курсового проектирования – неравномерность работы студента в течение семестра. Эта неравномерность создает существенную проблему, влияющую как на качество самого проектирования (учебного процесса), так и на загрузку преподавателя. Основным средством борьбы с этим явлением является обеспечение жесткого выполнения графика курсового проектирования. Системы управления обучением предлагают достаточный набор инструментов для организации этого процесса [24].

Производственная практика также является важнейшей составляющей подготовки. Каждый вид практики, применяемый в учебном процессе, является интегрирующим, выводящим на целостную профессиональную деятельность [25], [26]. Производственная практика, как правило, проводится после окончания семестра вне стен вуза и ограничивается по времени двумя – четырьмя неделями. В некоторых случаях на базе компьютерных подразделений вуза проводится учебная вычислительная практика [27]. Наконец, педагогическая практика в магистратуре может предусматривать проведение магистрантом в течение семестра обучения лабораторных или практических занятий со студентами. Одна из задач, которая возникает у организаторов при проведении практики – это обеспечение связи между руководителями практики (от вуза и от предприятия) и студентами. Эта задача с успехом может быть решена за счет применения средств системы управления обучением. Так, например, оказывается возможным ежедневный асинхронный контроль за деятельностью практиканта, обсуждение возникающих проблем с преподавателем и другими студентами, например, в форуме или чате, оперативное формирование и контроль отчётов по практике, а также аттестация.

Объем самостоятельной работы студентов в условиях Болонского процесса возрастает, в то время как объем аудиторной нагрузки неизбежно снижается. Скорее всего, в ближайшем будущем самостоятельная работа студентов станет наиболее распространенной и занимающей наибольшее учебное время студента формой организации учебного процесса. Нельзя не согласиться с высказанным в [28] утверждением: «Планирование, организация, методическое обеспечение и контроль самостоятельной работы являются одним из наиболее слабых мест в практике вузовского образования». Системы управления обучением в данном случае могут сыграть важнейшую роль и обеспечить оперативный доступ к знаниям, существующим в электронной форме, доставку необходимых материалов, тестирование и самотестирование знаний, исследования на виртуальном оборудование и многое другое [29]. Очевидно, что именно самостоятельная работа студента станет основой для интегрирования всех информационных систем вуза в единое целое [30]. Так, например, А.Ф. Сафина предлагает интегрировать управление самостоятельной работой с системой менеджмента качества вуза [31]. Особую роль самостоятельная работа студентов начинает играть при внедрении кредитно-рейтинговой системы [32] в практику работы вуза.

При использовании системы управления обучением основным средством контроля знаний студента может выступать тест. Важнейшей особенностью проведения тестирования в высшей школе является то, что его организацию и проведение осуществляет ведущий лектор по дисциплине, отчасти кафедра и, еще в меньшей степени, службы университета. Как следствие, возрастают трудозатраты всех перечисленных сторон, по крайней мере, на предварительном этапе. Рассчитывать на создание унифицированных в рамках высшей школы тестов по итогам изучения дисциплинам подготовки или по требуемым стандартами компетенциям (аналогов ЕГЭ средней школы) на настоящий момент не приходится. Поэтому возникает задача разработки методики организации автоматизированного тестирования, которую преподаватель высшей школы может освоить, использовать в своей практической деятельности и, в конечном итоге, уменьшить свои трудозатраты на проведение контроля знаний. Вопросам организации тестирования средствами Moodle посвящен целый ряд публикаций, среди которых отметим [7], [24], [33], [34], [35], [36].

В соответствии с новой редакцией стандарта образования, государственная итоговая аттестация (ГИА) – форма итогового контроля результатов обучения, выявляющая степень овладения выпускниками требуемыми компетенциями, и выполняемая за счет привлечения в том числе и внешних экспертов [37], обычно выступающих в роли председателей и членов аттестационных комиссий. В состав ГИА включается итоговый государственный экзамен и выполнение и защита выпускной квалификационной работы, организация и проведение которых также может быть автоматизировано за счет средств системы управления обучением.

Поскольку весь набор компетенций, которыми должен обладать выпускник, проверить за время ГИА оказывается невозможным хотя бы в силу их разно плановости, вузу придется сформировать портфолио выпускника, содержащие все результаты творческой работы студента в течение всего времени его обучения. Выполненные за время обучения контрольные и курсовые работы, рефераты, отчеты по лабораторным работам и практикам должны быть оценены по предварительно разработанной методике и сделаны доступными для заинтересованных лиц. Для этого их придется объединить в единый информационный блок, который часто называют портфолио, и дополнить его результатами измерений знаний и умений. Поэтому уже с начала обучения студента на первом курсе система управления обучением должна собирать и хранить отчетные материалы студентов с оценками преподавателей в специально созданном фонде оценочных средств. Очевидно, что для решения этой задачи потребуется еще одна информационная система, связанная с системой управления обучением. Ну и, наконец, если в вузе работает рейтинговая система, к моменту проведения ГИА должен быть сформирован итоговый рейтинг выпускников.

Методическая работа кафедры является важной и весьма трудоемкой составляющей, обеспечивающей выполнение собственно учебной работы. Она предусматривает разработку учебных планов и формирование целей и задач конкретных дисциплин, разработку и ежегодную корректировку учебно-методических комплексов дисциплин, обеспечение учебного процесса необходимой литературой и оборудованием, а также формирование необходимой отчетности.

На сегодняшний день трудоемкость выполняемой кафедрой методической работы приблизилась к трудоемкости учебной, а ее осязаемые результаты (программы дисциплин, учебники, учебные пособия и методические указания, контрольно-измерительные материалы, отчетные документы студентов и т.п.) по объему хранимого материала превысили все разумные пределы. Вполне естественным представляется переход кафедры на электронный документооборот с использованием электронной подписи, исключающий созданий и хранение твердых копий документов. Наличие системы управления обучением совместно с системой портфолио студента позволяет отказаться от бумажных документов и хранить всю отчетную документацию студентов в электронном виде. Существуют примеры разработки специальных модулей для системы управления обучением Moodle, реализующих электронный документооборот [38]. Системы управления обучением позволяет хранить актуальные методические материалы, предназначенные для студентов,

непосредственно на страницах изучаемых ими дисциплин. Служебные материалы кафедры также могут быть размещены на специальных страницах системы в ограниченном доступе.

Методическая работа кафедры, разработка и поддержка в актуальном состоянии образовательных программ, организация эффективной работы преподавателей традиционно регламентируется в вузе рядом внутренних документов, входящих, как правило, в систему управления качеством образования (СМКО). Эти процессы тесно связаны между собой и могут быть автоматизированы исходя из следующих основных принципов:

– любая информация в системе должна храниться в единственном экземпляре в виде информационных единиц и автоматизировано представляться в необходимых для сопровождения учебного процесса документах;

– за заполнение и актуальность отдельных информационных единиц должны быть четко закреплены ответственные сотрудники кафедры и руководители подразделений, чего следуют требования по разграничению прав доступа и защите информации в системе;

– использование сетевых технологий для внесения информации в систему;

– автоматическое формирование документов, обязательных для представления на портале вуза;

– обеспечение автоматизированного мониторинга состояния информационной среды на различных уровнях управления образовательным процессом.

Перечисленные принципы необходимо ведут к централизованному хранению данных не только по образовательным программам и их методическому обеспечению, но и о планировании работы и отчетности преподавателей. С учетом особенностей организационной структуры работы в данном направлении ведутся во многих вузах [38], [39], [40], [41], [42]. Известны решения лаборатории математического моделирования и информационных систем (ММИС) (http://mmis.ru) для автоматизации управления учебным процессом в образовательных организациях различного уровня.

Организационно-управленческая работа представляет собой еще одну составляющую деятельности кафедры, направленную на обеспечение учебного процесса. В статье [39] перечисляются следующие ее направления: расчёт учебной нагрузки и штата, разработка планов работы кафедры, разработка заданий, индивидуальных планов и составление отчётов о работе, организация проведения заседаний и совещаний кафедры, организация повышения квалификации профессорско-преподавательского состава, воспитательная работа со студентами, организация делопроизводства на кафедре, оценка качества подготовки студентов и эффективности работы сотрудников кафедры. Сюда можно добавить протоколов заседаний кафедры, учет и оформление отпусков и больничных листов сотрудников и некоторые другие позиции. Очевидно, что организационно-управленческая работа также требует привлечения информационных технологий.

Известно несколько вариантов автоматизации организационной деятельности. В работе [40] рассказывается о выполненном средствами Excel модуле расчета учебной нагрузки кафедры существующим в рамках автоматизированной системы «Электронная кафедра». В.В. Неретина [41] описывает комплекс разработанных на платформе 1С программных средств предназначенный для решения задач управления штатом профессорско-преподавательского состава кафедры, ведения перечней учебных дисциплин и учебных потоков, учета норм времени учебной работы, распределения учебной нагрузки между преподавателями кафедры, ведения данных об учебно-методической, научно-методической, научно-исследовательской и учебно-воспитательной деятельности преподавателей, создания планов годовой нагрузки преподавателя и индивидуальных планов работы преподавателя на предстоящий учебный год, формирование плана работы кафедры на будущий учебный год и отчета о выполненной работе кафедры за прошедший учебный год.

Существующая структура системы управления обучением также должна быть доработана на основании выявившихся в процессе ее эксплуатации недостатков. Одним из них является большая трудоемкость обслуживания системы. Так, подготовка к учебному году должна начинаться с ревизии структуры каталогов страниц дисциплин. Практика преподавания показывает, что учебный план даже одного направления обучения от одного года набора к другому меняется. Ручной режим коррекции не обеспечивает достаточной надежности. Кроме этого, в используемой нами версии Moodle приходится каждый раз вручную делать архивацию старых данных, подписывать студентов к страницам и, при необходимости, создавать новые и удалять старые страницы. Представляется целесообразным положить в основу структуры страниц дисциплин именно учебные планы дополняя их ежегодно новыми версиями и, при необходимости, корректируя. Кроме этого, вторым обязательным источником информации должен быть актуальный состав учебных групп. Имея эти данные можно на основании учебного плана текущего учебного года автоматически производить генерацию, заполнение и актуализацию страниц дисциплин.

Информационные технологии уже являются неотъемлемой составляющей высшего образования. На повестку дня выходит вопрос о системном их использовании. Общность решаемых задач и однотипность бизнес-процессов кафедр требуют интеграции уже используемых информационных систем в единый комплекс. В работе [42] описывается структура предполагаемой

информационной системы высшего учебного заведения. Если такая работа начинается с нуля, то с предложенной структурой нельзя не согласиться. С другой стороны, системы управления обучением, в частности Moodle, уже решают большинство задач учебного процесса. Объектно-ориентированный подход к созданию программного обеспечения позволяет проектировать общую структуру системы интегрируя в нее Moodle как самостоятельный класс и дополняя имеющуюся конфигурацию другими требуемыми классами, обеспечивающими необходимые кафедре бизнес-процессы.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриева А.В. Информационные технологии в бизнес-процессах кафедры вуза / А.В. Дмитриева, А.Г. Степанов // Высшее образование сегодня. 2014, №3, С. 42–46.
2. Байметова А.С. Нормирование и тарификация труда преподавателей вузов на основе информационной сложности / А.С. Байметова // Вестник Удмуртского университета, 2006, №2, С.192–198.
3. Курбатова М.В. Эффективный контракт в системе высшего образования РФ: теоретические подходы и особенности институционального проектирования // М.В. Курбатова, С.Н. Левин // Journal of institutional studies, 2013, Т. 1 №5, С.55–80.
4. Курбатова М.В. Новый государственный менеджмент в российской системе высшего профессионального образования / М.В. Курбатова // Научные труды Донецкого национального технического университета. Серия: экономическая. 2014, №2, С.36–45.
5. Довейко А.Б. Вузовский преподаватель: штрихи к портрету на фоне реформ / А.Б. Довейко // Социология, 2010, №2, С.175–184.
6. Верецкая А.И. Исследование образа жизни вузовских преподавателей / А.И. Верецкая, А.Б. Довейко, А.П. Дьяков, Е.Ю. Красова, Ю.Б. Матюшина, А.И. Стеценко // Вестник Воронежского государственного университета. Серия: проблемы высшего образования, 2011, №1, С.117–122.
7. Информационные технологии в работе кафедры / А.Н. Бабенков, В.С. Блюм, С.Д. Бодрунов и др. // под общ. ред. А.Г. Степанова. СПб.: ГУАП, 2014, 276с.
8. Григоров Г.А. Медиа-образовательное пространство на пересечении методологий философии образования и медиа-философии / Г.А. Григоров // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2013, №12–3 (38), С.54–57.
9. Макарова Н.В. Информатика в системе непрерывного образования. Монография / Н.В. Макарова, А.Г. Степанов // СПб.: Политехника, 2005, 338с.
10. Глотова М.Ю. Организация, поддержка и контроль образовательного процесса при преподавании в высшей школе на базе СДО Moodle / М.Ю. Глотова, Е.А. Самохвалова // Преподаватель XXI век, 2012, Т.1, №4, С.15–23.
11. Дистанционное обучение / ООО «Институт Консалтинга и Сертификации», 2007–2014 [В Интернете]. Available: http://www.icc-iso.ru/services/training/remote/. [Дата обращения: 31. 12. 2014].
12. Богомолов В.А. Обзор бесплатных систем управления обучением [В Интернете]. Available: http://ifets.ieee.org/russian/depository/v10_i3/html/9_bogomolov.htm. [Дата обращения: 01 01 2015].
13. Минацевич Е.С. Использование мультимедийных технологий в создании электронных конспектов лекций / Е.С. Минацевич // В кн. Формирование гуманитарной среды в вузе: инновационные образовательные технологии. Компетентностный подход, Пермь, 2014, Т.1, С.469–474.
14. Ощепкова О.В. Лекция-визуализация как активная форма обучения студентов / О.В. Ощепкова // Вестник Самарского юридического института, 2014, №1 (12), С.94–97.
15. Иванова Г.С. Особенности использования мультимедийных технологий при чтении лекций по программированию. / Г.С. Иванова // Наука и образование: электронное научно-техническое издание, 2014, №3, С.373–387.
16. Степанов К.С. Применение информационных технологий при обучении электротехническим дисциплинам / К.С. Степанов, Н.Г. Панкова // Инженерный вестник Дона, 2014, Т.29, №2, С.65–72.
17. Семенов В.И. Возможности мультимедийных презентаций в образовательном процессе высшей школы / В.И. Семенов, Е.В. Семенова и Н.И. Семенова // Современные проблемы науки и образования, 2013, №5, С.229–237.
18. Томилин А.К. Разработка и методика использования мультимедийных лекций / А.К. Томилин // Высшее образование сегодня. 2014, №9, С.3–6.
19. Космачев В.М. Организация дистанционного чтения лекций на основе Microsoft Office Live Meeting / В.М. Космачев, А.В. Михеев // Актуальные проблемы экономики и управления, 2014, №1 (1), С.71–75.
20. Лебедева Т.Е. Информационные технологии на практических занятиях в вузе / Т.Е. Лебедева // Высшее образование сегодня, 2007, №8, С.49–51.
21. Бобриков Б.Б. Компьютерные лабораторные работы по техническим дисциплинам / Б.Б. Бобриков, А.Н. Любин и В.Г. Смирнов // Известия Московского государственного технического университета МАМИ, 2013, Т.6, №1 (15), С.204–209.
22. Аскарова З.И. Дистанционная лабораторная работа как эффективная форма дистанционного обучения в техническом вузе. / З.И. Аскарова // Гуманитарные науки и образование, 2013, №3 (15). С.12–14.
23. Трэвис Д. LabVIEW для всех / Д. Трэвис, Д. Кринг. М.: ДМК Пресс, 2011, 903с.
24. Москалева О.И. Применение коллаборативных инструментов для организации и поддержки обучения студентов экономических специальностей / О.И. Москалева // Актуальные проблемы экономики и управления, 2014, №3 (3). С.85–91.
25. Полевая Н.М. Интеграция учебных дисциплин и различных видов практик в профессиональной подготовке по специальности «Социальная работа» / Н.М. Полевая, А.В. Лейфа // Вектор науки Тольяттинского государственного университета. Серия: Педагогика, психология, 2013, №1, С.195–200.
26. Лазарев Г.И. Ориентированное на практику обучение – ответ на требования внешней среды / Г.И. Лазарев // Высшее образование в России, 2012, №4, С.3–13.
27. Моисеев В.П. Методическое обеспечение учебной вычислительной практики / В.П. Моисеев // Вестник Московского городского педагогического университета. Серия: Информатика и информатизация образования, 2004, №3, С.117–123.
28. Атанов И.В. Самостоятельная работа студентов – важнейшая составляющая учебного процесса / И.В. Атанов, И.В. Капустин, М.В. Данилов // Вестник АПК Ставрополья, 2012, №1, С.4–6.
29. Анисимова Т.И. Организация самостоятельной работы бакалавров средствами дистанционного обучения / Т.И. Анисимова // Фундаментальные исследования, 2013, №11–4, С.747–750.
30. Николаева Л.В. Управление самостоятельной работой студентов в интерактивной информационно-образовательной среде / Л.В. Николаева // Вестник Бурятского государственного университета, 2011, №1, С.160–163.
31. Сафина А.Ф. Моделирование системы управления самостоятельной работой студентов в системе менеджмента качества вуза / А.Ф. Сафина // Высшее образование сегодня, 2014, №7, С.27–30.
32. Кадыров С.К. Управление самостоятельной работой студента при кредитной системе обучения / С.К. Кадыров // Вестник Челябинского государственного педагогического университета, 2011, №11, С.78–86.
33. Кравец О.Я. Информационное управление процессами многоуровневой индивидуализации обучения / О.Я. Кравец, О.Ю. Заславская и Р.В. Беляев // Вестник Российского университета дружбы народов. Серия: информатизация

образования. 2010, №1, С.72–80.
34. Медведева С.Н. Информационные технологии контроля и оценки знаний в системе дистанционного обучения Moodle / С.Н. Медведева, П.И. Тутубалин // Образовательные технологии и общество, 2012, Т.15, №1, С.555–566.
35. Колгатин А.Г. Вопросы качества процедур тестирования и интерпретации тестовых результатов в информационно-коммуникационной педагогической среде / А.Г. Колгатин, Л.С. Колгатина // Образовательные технологии и общество, 2013, Т.16, №1, С.575–585.
36. Хохлов Д.Г. Оценка уровня подготовки в системе электронного обучения программированию / Д.Г. Хохлов, З.Х. Захарова, А.Н. Захаров // Образовательные технологии и общество, 2012, Т.15, №1, С.537–554.
37. Эхов С.Ф. Новые требования к итоговой аттестации в условиях уровневой подготовки и реализации образовательных стандартов третьего поколения / С.Ф. Эхов // Universum: Вестник Герценовского университета, 2010, №8, С.64–65.
38. Назаров А.И. Совершенствование электронного документооборота кафедры биомедицинского профиля на базе LMS Moodle / А.И. Назаров // Инженерный вестник Дона, 2012, Т.22, №4–1 (22), С.27.
39. Григораш О.В. Инновации в организационно-методической работе на кафедре / О.В. Григораш, А.И. Трубилин. // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2013, №91, С.1888–1899.
40. Леонтьев А.Ю. Автоматическая система распределения учебной нагрузки с учётом квалификации преподавателей. / А.Ю. Леонтьев, Н.М. Василевский, А.И. Акмуллин // Ученые записки Казанской государственной академии ветеринарной медицины им. Н.Э. Баумана, 2013, Т.216, С.192–197.
41. Неретина В.В. Автоматизированная система документооборота структурных подразделений учебных заведений. / В.В. Неретина // Перспективы развития информационных технологий, 2013, №13, С.134–149.
42. Григорьева А.Л. Проектирование и создание модулей информационной системы университета / А.Л. Григорьева, Я.Ю. Григорьев // Интернет-журнал Науковедение, 2014, №2, С.105.

УДК 811.116.1

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАТИВНЫХ ТЕХНОЛОГИЙ НА ЗАНЯТИЯХ ПО РУССКОМУ ЯЗЫКУ

Колоколова Лидия Петровна
Стерлитамакский филиал Башкирского государственного университета
Россия, Республика Башкортостан, Стерлитамак, пр. Ленина, д. 49
e-mails: kollidia@rambler.ru

Аннотация: В статье рассмотрены информационно-коммуникативные технологии, активно применяемые в учебной деятельности при изложении нового материала, на этапе закрепления изученного материала, при контроле и проверке, а также при самостоятельной работе. Процесс технологизации ускоряет передачу и освоение знаний, способствует формированию языковой картины мира, обеспечивает взаимодействие преподавателя и обучаемого в современных системах открытого и дистанционного образования.

Ключевые слова: *информационно-коммуникативные технологии; компьютерное обучение; интерактивная доска; программное обеспечение.*

USING INFORMATION AND COMMUNICATION TECHNOLOGIES THE LESSONS OF THE RUSSIAN LANGUAGE

Lidia Kolokolova
Sterlitamak Branch of Bashkir state university
Russia, Republic of Bashkortostan, Sterlitamak, Lenin Prospect, 49

Abstract. The article presents information and communication technologies, actively used in the educational activity in describing new material, at the stage of consolidation of the material, at controls and examination, as well as independent work. Process technologizing accelerate the transfer of knowledge and learning, promotes formation of a language picture of the world, provides interaction the teacher and the student in modern systems of open and distance education.

Keywords: *Information and communication technologies; computer education; interactive whiteboard; software.*

Введение. В российской системе образования наблюдается устойчивый интерес исследователей к привлечению информационно-коммуникативных технологий в преподавание лингвистических дисциплин. Внедрение информационно-коммуникативных технологий (ИКТ) в образовательный процесс не столько насущная необходимость, сколько осознанный процесс технологизации рутинных процессов с целью высвобождения творческой энергии личности современного общества. Информационно-коммуникативные технологии в обучении русскому языку позволяют интегрировать в рамках одной программы тексты, графику, звук, анимацию, видеоклипы, высококачественные фотоизображения. Сфера использования информационно-коммуникативных технологий широка. Во-первых, названные технологии можно использовать при изучении нового материала: визуализация знаний (демонстрационно-энциклопедические программы, программы создания презентаций, интерактивная доска). Во-вторых, на этапе закрепления изученного материала

(программы-тренажеры). В-третьих, при контроле и проверке изученного (программы для тестирования и контроля). В-четвертых, при самостоятельной работе учащихся (программы-репетиторы, электронные энциклопедии, развивающие программы). Наконец, для индивидуальной тренировки конкретных способностей учащегося: внимания, памяти, мышления и т.п.

Таким образом, одной из наиболее важных задач, стоящих перед российской системой образования, является обеспечение доступности и качества образовательного процесса, итогом которого должно быть формирование конкурентоспособного выпускника. Данная цель не может быть достигнута без широкого внедрения, без опоры на современные информационные технологии в образовании.

С учетом актуального когнитивно-антропоцентрического взгляда на язык, в частности, и на весь комплекс гуманитарных наук, в целом, преподаватели-русисты считают возможным предложить некоторые новые требования и рекомендации к преподаванию русской словесности в школе и академических лингвистических курсов вузовской практике.

1. Преподавание словесности должно опираться прежде всего на классические тексты разных стилей и жанров, которые помимо фактуальной информации представляют определенную национальную культуру, особенности национальной картины мира, национального менталитета, в которых отражаются элементы духовной и материальной культуры народа в определенную историческую эпоху его существования.

2. Осуществлять преподавания словесности в соответствии с принципом системности, учить видеть в каждом отдельном факте языка сеть взаимосвязей его с фактами всех языковых уровней и экстралингвистическими категориями, понятиями и реалиями, которые получают отражение в данном языковом факте.

3. Ввести в лингвистический цикл предметов, преподаваемых в высших учебных заведениях, круг дисциплин, связанных с новыми направлениями современной филологии: лингвосемиотику, лингвокультурологию, риторику, теорию коммуникации, прикладную лингвистику.

Методологически внедрение ИКТ в процесс обучения ускоряет передачу и освоение знаний и способствует формированию языковой картины мира. Важным качеством современных ИКТ является их универсальность: они могут быть основой в организации любой деятельности, связанной информационным обменом, основой в создании общего информационного языкового пространства.

Наибольшую популярность среди технических приложений лингвистики получило компьютерное обучение. Компьютер является многофункциональным помощником, хорошим методическим инструментом наряду с другими средствами обучения. Актуальность компьютерных технологий в преподавании русской словесности налицо, так как новые условия, непринужденная обстановка, общение с компьютером, одобрение электронного помощника результатов труда имеют позитивную оценку. Студенты с разной степенью грамотности сосредотачиваются на ключевых моментах, так как машина идет вместе со студентом от незнания к знанию, акцентируя внимание на неусвоенном материале.

Для активизации учебной деятельности студентов создаются электронные учебники, позволяющие самостоятельно приобретать навыки грамотного письма, проверять собственные знания и подготавливаться к различным типам контрольных работ по русского языку.

Одним из последних по времени появления среди новых технических приложений лингвистики явилось применение интерактивных электронных досок. В процессе проведения учебных занятий использование интерактивной доски выводит на новый уровень подачу материала, создается комфортная среда при объяснении учебного материала и поддерживается атмосфера интересной познавательной беседы при обсуждении языковых явлений. В частности, в преподавании курса «Фонетическая система современного русского литературного языка» ключевым понятием является фонетическая транскрипция, представляющая собой передачу на письме графемами-буквами и специальными дополнительными знаками звучания различных по величине отрезков живой речи. Потребность в транскрипции была обусловлена зарождением сравнительно-исторического языкознания и развитием фонетики как науки. В специальных лингвистических трудах обычно применяется транскрипция Международной фонетической ассоциации, основанная на латинской графической системе. Бесспорно, используя интерактивные технические средства, можно детально представить фонетическое письмо и познакомить студентов с системой важных знаков транскрипции. Кроме того, интерактивная доска может быть использована при изучении артикуляционно-акустической системы современного русского литературного языка. Например, артикуляционная характеристика системы консонантизма предполагает следующие артикуляционные признаки:

1) характеристика согласных звуков по участию голоса и шума (сонорные и шумные);

2) характеристика согласных звуков по участию голосовых связок (шумные звонкие и шумные глухие: [б] - [п], [в] - [ф], [г] - [к], [з] – [с] и т.п);

3) характеристика согласных звуков по способу образования шума в полости рта (щелевые, смычные, аффрикаты (смычно-щелевые));

4) характеристика согласных звуков по месту образования шума в полости рта (переднеязычные (зубные, нёбные), среднеязычные, заднеязычные);

5) характеристика согласных звуков по наличию/отсутствию палатализации (мягкие и твердые: [б] - [б’], [в] - [в’], [г] - [г’], [д] - [д’] и т.п.).

Таким образом, предложенная информация на занятиях по «Фонетике» современного русского литературного языка будет способствовать образному, зрительному восприятию учебного материала.

При изучении лексической системы современного русского литературного языка информационно-технические средства могут быть использованы при знакомстве с терминологическим аппаратом. В ходе занятий по разделу «Лексикология» студент должен овладеть определенным запасом довольно сложных лингвистических терминов, уметь профессионально квалифицировать языковые факты, формировать лингвистическое чутьё. Терминологический словарь составляет теоретическую основу изучаемой дисциплины, включает в себя словарные статьи по наиболее частотным терминам с дефинициями по теме «Лексикология. Фразеология. Лексикография», встречающимся в вузовских учебниках лингвистического цикла, лекционных курсах, на практических и семинарских занятиях, при изучении студентами курса сравнительной лексикологии и в школьной практике, при чтении периодических изданий не только популярных, но и академического типа. Помимо толкования терминов в терминологическом словаре приводятся примеры из ряда языков, особенно из истории развития русского языка, в его литературном варианте, просторечии и диалектах. Особенностью данного словаря является то, что он многофункционален (перевод терминов на изучаемые языки предваряется этимологическими сведениями). Например, в словарной статье «основные признаки слова (по теории А.И. Смирницкого)» представлены фонетические, лексико-грамматические и лексико-семантические признаки слова. В свою очередь, к фонетическим признакам слова относятся следующие особенности слова: 1) цельность и единооформленность, 2) фонетическая оформленность, 3) недвуударность, 4) непроницаемость, 5) постоянство звучания и значения. Лексико-грамматическим признакам слова включают такие свойства слова, как 1) изолируемость, 2) цельность и единооформленность, 3) лексико-грамматическая отнесенность. К лексико-семантическим признакам относят 1) фразеологичность, 2) номинативность, 3) воспроизводимость, 4) семантическая валентность.

Все указанные признаки в терминологическом словаре представляют собой семантическое пространство, которое студент должен рассмотреть в течение определенного периода времени и использовать данную информацию на практических и семинарских занятиях. Более того, терминологический словарь содержит порядок и образец лексических, фразеологических и лексикографических анализов, используемых студентами при выполнении лабораторных работ.

Технические средства также успешно находят применение при составлении словарей разного типа. Например, по теме «Лексикография» важно учитывать следующие этапы работы: 1) предмет, объект, задачи изучаемой проблемы, 2) словарь, структура словаря, 3) понятие словарной статьи, структура словарной статьи, 4) функции словарей, 5) типология словарей, 6) лексикографический анализ слова. Интерактивная доска даёт возможность представить исследовательскую работу в целом и затем поэтапно рассматривать каждый отдельный информационный блок. Особенно этот вид деятельности характерен при анализе схемы комплексного лексикографического анализа, включающего следующие виды деятельности: 1) дать полное название словаря, 2) указать, выходные данные (автор (ы), год издания, место издания, издательство), 3) определить объект описания, 4) охарактеризовать структуру словарных статей и их содержание, 5) определить принцип построения словаря, 6) определить структуру словаря, 7) определить, на кого рассчитан словарь, 8) охарактеризовать объём словаря и специфику его оформления: таблицы, схемы, карты, иллюстрации, фото ит.п., 9) описать словарную статью.

Более того, интерактивная доска позволяет демонстрировать слайды и видео, рисовать и чертить различные схемы, вносить любые изменения и сохранять их в виде компьютерных файлов для дальнейшего редактирования.

Совершенно очевидно, что информационные и коммуникационные технологии (ИКТ) – это широкий спектр цифровых технологий, используемых для создания, передачи и распространения информации и оказания услуг (компьютерное оборудование, программное обеспечение, телефонные линии, сотовая связь, электронная почта, сотовые и спутниковые технологии, сети беспроводной и кабельной связи, мультимедийные средства.

Примером успешной реализации ИКТ в современном учебном процессе стало появление Интернета – всемирной компьютерной передачи с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю. Технология Интернет как среда коммуникации является посредником во включении студента в сетевые структуры, на основе которого он получает возможность эффективно использовать информацию, предоставляя ее заинтересованным людям в кратчайшие сроки.

Технические средства активно используются в рамках дисциплины «Русский язык и культура речи» при изучении таких тем, как орфоэпические, акцентологические, морфологические,

синтаксические, и лексические нормы. Более того, информационно-коммуникативные технологии используются при составлении тестовых заданий.

Прорыв в области ИКТ, происходящий в настоящее время, заставляет пересматривать вопросы организации информационного обеспечения научно-исследовательской деятельности. Можно выделить несколько возможностей использования информационных технологий:

1) для поиска литературы

а) в электронном каталоге библиотеки учебного заведения;

б) в Internet с применением браузеров типа Internet Explorer, Mozilla Firefox и др., различных поисковых машин (Yandex.ru, Rambler.ru, Mail.ru, Aport.ru, Google.ru, Metabot.ru, Search.com, Yahoo.com, Lycos.com и т.д.);

2) для работы с литературой в ходе реферирования, конспектирования, аннотирования, цитирования и т.д.;

3) для автоматического перевода текстов с помощью программ-переводчиков (PROMT XT), с использованием электронных словарей (Abby Lingvo 7.0.);

4) для хранения и накопления информации (CD-, DVD-диски, внешние накопители на магнитных дисках, Flash-диски);

5) для планирования процесса исследования (система управления Microsoft Outlook);

6) для общения с ведущими специалистами (Internet, электронная почта);

7) для обработки и воспроизведения графики и звука (проигрыватели Microsoft Media Player, WinAmp, Apollo, WinDVD, zplayer, программы для просмотра изображений ACD See, PhotoShop, CorelDraw, программы для создания схем, чертежей и графиков Visio) и др.;

8) для пропаганды и внедрения результатов исследования (выступления в видеофорумах, телемостах, публикации в СМИ, Интернет).

Также информационные технологии могут оказать помощь в создании по результатам исследования учебных и воспитательных фильмов, мультфильмов, передач, роликов социальной рекламы для телевидения, обучающих компьютерных программ, игр, интерактивных путешествий, энциклопедий и т.д.

Совершенно очевидно, эффективность обучения может быть значительно повышена с помощью ИКТ, применяемых в различных оптимальных для данных занятий сочетаниях с другими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Колоколова Л.П. Современный русский язык. Лексикология. Фразеология. Лексикография: Учебное пособие для филол. фак. вузов. – СПб: Политехника-сервис, 2012. 147 с.
2. Современный русский литературный язык и методика его преподавания: Учебный словарь. – М.: ИПЦ «Маска», 2012, 383 с.

УДК 37:01:007

ПОИСК СТРАТЕГИЙ КОНВЕРГЕНЦИИ НАУКИ ВЫСОКИХ ТЕХНОЛОГИЙ И ОБРАЗОВАТЕЛЬНЫХТЕХНОЛОГИЙ НОВОГО ТИПА

Лаптев Владимир Валентинович, Носкова Татьяна Николаевна, Флегонтов Александр Владимирович, Гавронская Юлия Юрьевна, Пиотровская Ксения Раймондовна,
Российский государственный педагогический университет им. А.И. Герцена,
Россия, Санкт-Петербург, н.р. Мойки, д. 48,
e-mails: laptev@herzen.spb.ru, flegontoff@yandex.ru, noskovatn@gmail.com,
gavronskaya@yandex.ru, krp62@mail.ru

Аннотация: Анализируется современные тенденции в развитии науки и образовании. Формулируется понятие «высокотехнологичная образовательная среда». Исследуется вопрос о цифровых компетенциях 21 века.

Ключевые слова: *цифровые компетенции; высокотехнологичная образовательная среда; трансдисциплинарность; информационно-коммуникативные технологии.*

THE UNDERSTANDING OF CONVERGENCEs of HIGH-TECH SCIENCE AND NEW TyPE EDUCATIONAL ENVIRONMENT

Vladimir Laptev, Tatiana Noskova, Alexandr Flegontov, Yulia Gavronskaya, Xenia Piotrowska,
Herzen State PedagogicalUniversity of Russia,
Russia,St.Petersburg, r. Mojka 48,
e-mails: laptev@herzen.spb.ru, flegontoff@yandex.ru, noskovatn@gmail.com,
gavronskaya@yandex.ru, krp62@mail.ru

Abstracts: Analyzes the complex features that make manifest innovative properties of modern science. The concept of "high-tech" educational environment is formulated.The system of 21-st century digital competences is under discussion.

Keywords: *digital competences; information and communication technologies; information educational environment; a high-tech network educational environment.*

Активно нарастающая информатизация деятельности человека, с одной стороны, и выдвигаемые инновационной экономикой требования к современному специалисту, с другой, предопределяют неизбежный переход к новым приемам работы со знаковыми системами в науке и образовании.

Исследования в области философии и методологии науки XX века фиксируют изменения не только оснований науки [2], но и организации самой науки. Процесс формирования качественно новой стадии развития науки и техники, а также их взаимодействий с обществом, выразился в формировании так называемой технонауки. В этот период, вычислительное и информационное моделирование превращается в самостоятельный компонент научного метода наряду с экспериментом и теорией, а математическое моделирование в научных исследованиях рассматривается как самостоятельный метод познания. Появляются новые области: компьютерная алгебра (символьные вычисления), вычислительный эксперимент, имитационное моделирование, квантовые вычисления. Повсеместная информатизация способствует тотальной рационализации и автоматизации научной деятельности. Меняется само видение мира и язык науки. Выделяются принципиально иные интеллектуальные способы решения профессиональных задач и формы представления, и извлечения знаний [4].

Все перечисленные выше изменения в науке приводят к созданию новейшего междисциплинарного (не только естественнонаучного и технологического, но и социально-гуманитарного) научного знания, а также к формированию особой электронной среды обитания, которая опирается на работу технологий нового типа, называемых «высокими», причем инвариантом «высоты» той или иной технологии считают снижение степени участия человека в технологическом процессе любой природы. Поскольку базовыми для высоких технологий выступают именно технологии информационные, то выделяются основные стадии, которые вскрывают информационную природу создания технологий нового типа:

– стадия технологического знания, включающая в себя такие этапы информационного процесса, как генерация, рецепция, кодирование, хранение информации;

– стадия технологического процесса – этапы кодирования, передачи информации;

– стадия репликации продуктов технологии – этап тиражирования и редупликации информации.

Благодаря развитию средств вычислительной техники восприятие становится все более косвенным, превращая реальность в опосредованную телетехнологию [1]. В том числе, это касается и способов общения в современном научном и образовательном сообществах, которые, активно используя аппарат телеконференций и интернет-форумов, становятся все более интерактивно дистанционным. Поэтому для реалий сегодняшнего образования важно, что к высоким технологиям наряду с наиболее новыми и прогрессивными наукоёмкими отраслями промышленности, относят также социальные технологии, например, системы распространения новостей, технологии коллективной работы и обучения, и все больше говорят о высоких социальных технологиях.

Сказанное выше приводит к неизбежной генерации иных способов взаимодействия с информационными средами и формированию нового мышления, что требует поиска подходов к решению описанных выше задач и осознания новых требований к выпускникам вузов. Проблемы инноваций в информатизации образовательной деятельности, IT-исследований в гуманитарных и естественнонаучных областях, а также социально-культурные эффекты информатизации должны быть рассмотрены комбинированно: с трансдисциплинарных и психодидактических позиций к построению образовательных сред нового типа.

Разрабатываемая нами концепция высокотехнологичной информационной образовательной среды (ВТИОС) опирается на следующие положения [3]:

– в соответствии с трендами развития глобальной, толерантной среды взаимодействий ВТИОС расширяет и обогащает традиционную аудиторную среду взаимодействий;

– ход процесса обучения изменятся под влиянием новых качественных аспектов, а именно в связи со смещением центра образовательных взаимодействий от педагога к обучающимся, которые активно взаимодействуют с ресурсами среды, с педагогом и между собой;

– формирование новой педагогической методологии, позволяет учащемуся выстраивать и реализовать персонализированную стратегию «обучение через жизнь» в обществе знаний.

– педагог организует, стимулирует и сопровождает этот нелинейный, многовариантный образовательный процесс, опираясь на логику сетевого взаимодействия;

– виртуальная часть среды, становясь новым объектом профессиональной деятельности, позволяет вырабатывать новые технологии внеаудиторной самостоятельной деятельности обучающихся, поддерживать современный ход информационных и коммуникационных процессов, а также современный образовательной запрос молодежи, нацеленный на актуализацию сообществ обмена знаниями и ценностями.

Поэтому высокотехнологичная информационная образовательная среда понимается нами как человеко-машинная нелинейная, многовариантная образовательная система, обеспечивающая кардинальное изменение форм и форматов представления и функционирования знаний, в соответствии с актуальными трендами глобальной среды взаимодействий, с предоставлением субъекту широкого выбора из насыщенной ресурсной базы и различных способов коммуникации при решении образовательных задач и формировании системы компетенций.

Предполагается, что формирование высокотехнологичной информационной образовательной среды должно позволить обеспечить с помощью информационных и коммуникационных процессов связь традиционных и виртуальных, электронных форматов знаний, и тем самым удастся достичь качественных позитивных сдвигов в решении научных, образовательных, социальных и культурных задач современного университета.

Во многих случаях информационная образовательная среда является виртуальной надстройкой, структурирующей современные способы организации информационного сопровождения образовательного процесса. Ее облик имеет тенденцию к персонализации и должен иметь следующую примерную инфраструктуру:

– персональные обучающие среды (PLE): WordPres, Blogger, Google Sites,Yola);
– сообщества обменазнаниями (V-class.ru, VebinarExpert.ru, Skype.com/intl/ru, VZOchat.com/ru/);
– совместная информационная деятельность Google Sites, Wiki, Windows Live Space;
– дистанционное обучение (LMS): Moodle, Прометей, Web Tutor, средства для организации виртуальных лабораторий и т.п.;
– массовые открытые онлайн-курсы (MOOC): Coursera, EdX,Udacity;
– сетевые депозитарии: DocsGoogle, FriendFeed, YouTube, SlideShare;
– аудиовизуальные средства: Skype, GoogleTalk, AnyMeeting.

При этом информационно-коммуникационным базисом всех выделенных областей является Интернет, с его традиционными и инновационными сервисами Web 2.0 и Web3.0.

В то же время, новые требования к профессиональной подготовке снова и снова требуют пересмотра системы компетенций, которыми должен обладать специалист в 21 веке [6], [7]. В последние годы в системе компетенций 21 века появилась компетенция нового типа – цифровая компетенция, которая предполагает наличие высокого уровня информационной грамотности и связанных с нею понятий: сквозные компетенции, медиаграмотность, электронная грамотность, компьютерная грамотность, цифровая грамотность, визуальная грамотность и т.д. (рисунок 1).

Рис. 1. Соотношение понятий цифровые компетенциии грамотностей различного типа

Современное определение цифровой компетенции опирается на конвергентное понимание развития процессов, протекающих в области науки и техники, а также в социуме [5].

Если первоначально, цифровая грамотность в основном понималась как владение средствами вычислительной техники и языками программирования, а также их теоретическими основаниями, то в настоящее время цифровая грамотность подразумевает способность к пониманию медиа с целью поиска и критического извлечения информации (с широким привлечением возможностей Интернета), а также взаимодействие с помощью различных цифровых инструментов и мобильных приложений. Задачи воспитания этих компетенций относятся к самым разным дисциплинам: медиа исследования; информационные науки; программирование, теория коммуникации и т.д.

На рисунке показано, что сегодня Интернет-, ИКТ-, медиа – и информационная грамотности содержат цифровой компонент, поэтому цифровая грамотность обогащается новым значением и инструментарием, полученными вследствие недавнего технологического скачка и конвергенционных тенденций развития знания. По мнению британских исследователей цифровая компетенция как интеграция ИКТ- и информационной компетенции стимулирует не столько развитие цифровых навыков, сколько способствует развитию социализации и критического мышления [8]. Особое значение здесь имеет связь цифровых компетенций с компетенциями общекультурного цикла.

Общую систему отношений цифровых компетенций и компетенций мы представляем в виде радиально вложенных колец (рисунок 2).

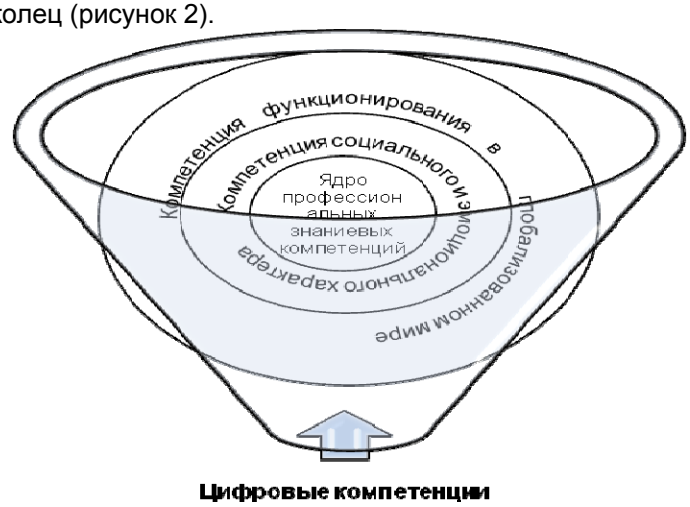


Рис. 2. Влияние цифровых компетенций на общую систему компетенций

Знания и навыки в профессиональной сфере образуют внутреннее ценностное ядро в компетентностном ряду 21-го века. Именно они во многом влияют на формирование убеждений, взглядов и действий человека и подкрепляются кольцом цифровых компетенций, которые в свою очередь помогают сформировать компетенции следующих уровней. Следующее кольцо содержит компетенции социального и эмоционального характера – навыки, необходимые молодому человеку для распознавания и контроля над своими эмоциями, развития заботы о других, принятия ответственных решений, налаживания отношений, а также оперативной и эффективной обработки сложных ситуаций.

Внешнее кольцо компетенций на рисунке представляет формирующуюся систему компетенций, необходимых для функционирования в глобализованном мире, основными чертами которого являются: гражданская грамотность, информированность мировой общественности и кросс-культурные навыки общения, критичность и изобретательность мышления, навыки в области осуществления коммуникации, сотрудничества и работы с информацией.

Каждый из участников учебного процесса (педагог, администратор, учащийся) имеет собственную, уточненную систему цифровых компетенций (рисунок 3). Важно, что именно совместное, конвергентное воспитание этих компетенций позволит формировать специалистов 21 века, способных эффективно и безопасно работать в цифровую эпоху.

Педагогам информационного века предстоит освоить виртуальную образовательную среду как новую площадку своей профессиональной деятельности, и для этого овладеть передовой педагогической и информационной методологией, инновационными подходами и методиками образовательных взаимодействий.

В этом случае, после осознания иных психологических оснований цифровой деятельности в этой среде, будет осуществлен переход от массового, поточного обучения к субъектно-ориентированному процессу, с учетом современного информационного и коммуникационного поведения молодежи.

Рис. 3. Схема цифровых компетенций XXI века для различных категорий участников учебного процесса

Кардинальные изменения в самой системе образования, основанные на переходе от технократического к антропоцентрическому подходу, позволят преодолеть ее инерционность, переориентировав на воспроизводство человеческого капитала на основе высоких технологий с применением современных образовательных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Дрейфус Х. Чего не могут вычислительные машины: Критика искусственного разума. М.:Изд. «Прогресс», 1978, 200с.
2. Жукова Е.А. Влияние высоких технологий на взаимодействия современной науки и образования // Философия образования. – 2005, №3 (14), С.207–214.
3. Носкова Т.Н. Педагогическая сущность виртуальной образовательной среды // Известия Российского государственного педагогического университета имени А.И. Герцена, СПб., 2014, №167, С.183–194.
4. Флегонтов А.В. Hi-Tech: динамика взаимодействий науки и образования // Известия Российского государственного педагогического университета им. А.И. Герцена, СПб., 2014, №167, С.134–142.
5. Ala-Mutka, K. Mapping Digital Competence: Towards a Conceptual Understanding // Joint Research Centre – Institute for Prospective Technological Studies. Luxembourg: Publications Office of the European Union, 2011. Электрон. дан. – Режим доступа: http: //ipts.jrc.ec.europa.eu/publications/pub.cfm?id=4699 (дата обращения: 11.01.2015).
6. Ferrari An., Punie Yv., Redecker Chr. Understanding Digital Competence in the 21st Century: An Analysis of Current Frameworks //21st Century Learning for 21st Century Skills. Lecture Notes in Computer ScienceVolume 7563, 2012, pp.79–92.
7. Janssen J., Stoyanov Sl., Ferrari An., Punie Yv., Pannekeet K., Sloep P. Experts' views on digital competence: Commonalities and differences. //Computers & Education, V8, №68, Pergamon, 2013, pp.473–481.
8. Newton Th. A review of digital literacy in 0 – 16 year olds: evidence, developmental models, and recommendations. London: Becta, 2008, Электрон. дан. – Режим доступа: http://www.timmuslimited.co.uk/archives/117 (дата обращения: 19.01.2015).

УДК 378.02:37.016

ОПЫТ ИСПОЛЬЗОВАНИЯ ОБРАЗОВАТЕЛЬНЫХ СЕТЕВЫХ СООБЩЕСТВ НА ОСНОВЕ БЛОГОВ ПРИ ОБУЧЕНИИ СТУДЕНТОВ ДИСЦИПЛИНЕ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Моглан Диана Васильевна[1], Абрамян Геннадий Владимирович[2],
[1] Бельцкий государственный университет имени Алеку Руссо,
Республика Молдова, Бельцы, ул. Пушкина, д. 38,
[2]Российский государственный педагогический университет им. А.И. Герцена,
Россия, Санкт-Петербург, наб. Реки Мойки, д. 48,
e-mails: di_2008@mail.ru, abrgv@rambler.ru

Аннотация: В статье представлен опыт использования образовательных сетевых сообществ на основе блогов при обучении студентов дисциплине «Информационные технологии». Раскрывается понятие «образовательное сетевое сообщество» и обосновываются образовательные возможности учебных блогов в процессе реализации учебных проектов в образовательных сетевых сообществах вузов.

Ключевые слова: *образовательное сетевое сообщество; учебный блог; работа в группе; проектная деятельность.*

EXPERIENCE OF USING OF EDUCATIONAL NETWORK COMMUNITIES BASED ON BLOGS IN TEACHING STUDENTS OF THE DISCIPLINE "INFORMATION TECHNOLOGIES"

Diana Moglan[1], Gennady Abramyan[2],
[1]Alecu Russo Balti State University,
Republic of Moldova, Balti, Puskin str., 38,
[2]Herzen State Pedagogical University of Russia,
Russia, St. Petersburg, Moika Emb., 48,
e-mails: di_2008@mail.ru, abrgv@rambler.ru

Abstract: The article presents the experience of using educational network of community-based blogs to train students in the discipline "Information technologies". The definition of "educational network community" and substantiates the educational blogs in the process of implementing educational projects in the educational network community universities.

Keywords: *educational network community; education blog; teamwork; project activity.*

Основополагающими факторами успешности обучения студентов информационным технологиям (ИТ) является соответствие применяемых педагогических технологий современному уровню развития инфраструктуры информатизации образования и компьютерных сетей [1].

Особенности использования современных сетевых инфокоммуникационных технологий в свою очередь, требует разработки новых дидактических подходов к преподаванию дисциплины «Информационные технологии» [2] с учетом современных тенденций развития как уже сложившихся и «традиционных» ИТ, так и относительно инновационных систем глобальных цифровых образовательных коммуникаций [3] в том числе и на основе учебных блогов.

Как отмечает И.Н. Аржанов [4], в настоящее время информатика, являющаяся одной из фундаментальных областей научного знания, формирует системно-информационный подход к анализу окружающего мира и изучает информационные процессы, методы и средства получения, преобразования, передачи, хранения и использования информации. Стремительно развивается и постоянно расширяется область практической деятельности человека, связанная с использованием информационных технологий. Поэтому методика преподавания информатики требует постоянной модификации с учетом ее содержательной направленности и постоянной новизны, обусловленной современным информационным взрывом [4].

С учетом того, что аспекты обучения информатике с использованием глобальной сети Интернет изучены недостаточно полно [5], в настоящее время актуальным является внедрение в обучение ИТ современных и эффективных Интернет-технологий на основе сервисов Веб 2.0 и прежде всего – блог-технологий.

П.В. Сысоев [6] определяет *блог-технологию* как одну из технологий Веб 2.0, которая позволяет любому пользователю сети Интернет создать личную страницу, блог (от англ. blog или weblog), в виде дневника или журнала. Автор отмечает следующие дидактические свойства блога:

– публичность (блоги доступы всем участникам проекта, находящимся на расстоянии друг от друга);

– линейность (изменения и дополнения размещаются в хронологическом порядке);

– авторство и модерация (блогам присуще единоличное авторство, модерация блога осуществляется его автором);

– мультимедийность (возможность использования при создании контента блога материалов разного формата: текстового, графического, фото-, видео-, аудиоматериала).

Кроме того, блог определяется как информационное пространство в сети Интернет, где пользователь (блоггер) может регулярно публиковать различную информацию (текстовую, аудио/видео, изображения и т.д.), организуя тем самым сетевое сообщество для интерактивного общения пользователей [7], [8]. Следовательно, блоги могут стать удобной площадкой для организации обсуждений, посредством которого можно обеспечить устойчивую обратную связь и необходимый уровень индивидуализации и дифференциации обучения.

И. Фролов [9] считает необходимым подчеркнуть, что, разработав сетевую среду на основе блогов и внедрив ее в практику образовательных учреждений, можно гарантировать повышение качества образованности выпускников и повышение самообразования преподавателей.

Д.А. Иванченко [10] отмечает, что коммуникационный потенциал и возможности, предоставляемые блог-технологиями, позволяют по-новому подойти к решению таких вопросов организации дистанционного обучения, как:

– организация личного информационного пространства преподавателей и учащихся, в котором суммируются все документы и сообщения пользователя, хранятся в одном месте, что не только позволяет осуществлять кросспостинг (публикацию сообщения более чем в одно сообщество), но и облегчает работу с накопленными данными;

– организация открытых и закрытых сообществ для коллективного обсуждения различных вопросов и осуществления совместной работы под наблюдением модератора (преподавателя), что существенно расширяет эффективность групповой учебной деятельности;

– создание электронных и медиабиблиотек, в состав которых будут включены каталогизированные тематические базы обучающих, справочных, иллюстративных и других документов и данных для обеспечения адресного поиска и свободного сетевого доступа;

– обеспечение оперативной и надежной связи между учащимся и преподавателем для решения вопросов, получения ответов, обсуждения текущих проблем и организационных моментов;

– удобство добавления, чтения и поиска нужных сообщений предоставляет возможность разворачивания конструктивных дискуссий, которые являются неотъемлемой частью педагогического процесса;

– предоставление учащимся возможности обмена информацией друг с другом для само– и взаимообучения;

– использование электронных конспектов и лекций, когда обучающимся пересылаются тексты в электронном виде, выдержки из рекомендованной литературы и т.п., а затем проводятся групповые консультации;

– применение в учебном процессе тестов и опросов, позволяющих выявить промежуточный уровень знаний или определить отношение учащихся к какой-либо проблеме и т.д.

По мнению Е.В. Лазуткиной [11], блоги могут быть использованы в преподавании любой университетской дисциплины. Они служат не только средством организации процесса обучения и общения преподавателей и студентов, но и предоставляют студентам возможность поделиться своими размышлениями, реализовать свой творческий потенциал, обменяться интересной информацией.

Анализ образовательных возможностей блог-технологий позволил установить, что при помощи сервисов Веб 2.0 – блог-технологий – можно построить эффективную, удобную и простую в использовании образовательную среду в форме сетевого сообщества. Исходя из того, что деятельность студентов и преподавателя в сетевом сообществе будет связана с решением образовательных задач, можно определить такие сообщества как образовательные, существование и деятельность которых обусловлена как педагогическими технологиями, так и сетевыми технологиями Интернета. Образовательные сетевые сообщества – это сообщества сети Интернет, деятельность которых направлена на реализацию образовательных задач по отношению к обучаемым и педагогам как членам сообщества [12].

Учебная деятельность в сетевых сообществах предоставляет возможность получить доступ к разнообразной информации и опыту других людей, что позволяет повысить качество учебного процесса [13]. В ходе такого обучения формируется опыт совместной деятельности и приобретаются новые знания. Кроме того, при выборе правильной стратегии организации и управления сетевым сообществом в процессе дистанционного обучения в результате совместной деятельности преподавателей и студентов будут решены основные педагогические задачи, а также повышен личностный рост учащихся, выражающийся в появлении новых навыков и умений, необходимых для самообучения и саморазвития [14]. В целях проверки образовательных возможностей сетевого сообщества, а также фактического осуществления интернет-поддержки образовательного процесса с помощью сетевого сообщества, реализуемого в Бельцком государственном университете им. А. Руссо Республики Молдова, нами был проведен педагогический эксперимент в ходе обучения дисциплине «Информационные технологии» студентов педагогического образования (профиль «Информатика»). В проведенном эксперименте для обеспечения доступа к информационным ресурсам дисциплины и обмена информацией между студентами и преподавателем были использованы сервисы Веб 2.0 – блоги, с помощью которых стало возможным создание образовательного сетевого сообщества. Это позволило обеспечить совместную сетевую деятельность студентов и преподавателя, направленную на решение учебных задач, совместное обсуждение возникающих проблем, обмен опытом, информацией и ресурсами по учебной дисциплине, развитие познавательной активности студентов [15]. Построение и деятельность образовательного сетевого сообщества осуществляется в несколько этапов:

I этап – социализация (первая неделя обучения). Цель данного этапа состоит в более близком знакомстве студентов друг с другом, выборе предпочитаемых стилей обучения, раскрытие преобладающих способностей и черт характера у каждого, обнаружении качеств лидерства, создании чувства принадлежности к образовательному сообществу. Основываясь на отобранной информации из персональных карточек, заполненных студентами, преподаватель распределяет студентов по группам для работы над индивидуальными проектами. Опыт показал, что на формирование состава групп влияют личные предпочтения студентов, которые могут привести к появлению социокогнитивного конфликта. Для разрешения подобной ситуации на данном этапе мы проводили очные собрания, которые способствовали урегулированию сложных ситуаций и снижали уровни конфликтности.

II этап – сотрудничество (6 недель обучения). Цель данного этапа заключалась в деятельности над проектом и «сплочении» команды через совместную работу. Данный этап был разделен на несколько последовательных фаз: а) электронный брейнсторминг («мозговой штурм»), б) личный зачет идей, в) дебаты и коллективный зачет идей, г) коллективная разработка проекта.

В рамках электронного «мозгового штурма» студенты, используя имеющиеся средства, результаты личных поисков, собственные знания и накопленный опыт за период обучения и изучения данной дисциплины, формулируют как можно больше идей относительно способа реализации проекта. Предварительно студенты знакомятся с классическими правилами «мозгового штурма».

Эксперимент проведенный авторами на кафедре математики и информатики Бельцкого государственного университета им. А. Руссо показал, что процесс формулирования и генерирования идей затруднителен для студентов. В традиционном варианте, когда соответствующая деятельность происходит в аудитории, а идеи формулируются словесно, «мозговой штурм» терпит неудачу сразу на первом этапе. Причины неудач, на наш взгляд, обычно связанны с двумя основными проблемами:

– сокращение времени, выделенного для формулирования/генерирования идей, которое должно быть разделено между студентами-коллегами группы;

– некоторые студенты испытывают затруднения, страхи, боязнь публично ошибиться в высказывании своих идей на широкую аудиторию.

Технология электронного «мозгового штурма» в некоторой степени исключает данные проблемы, так как студент получает возможность в любой момент времени сформулировать идею и отправить ее на сервер. В то же время традиционный вариант формулирования/генерирования идей имеет свое преимущество, состоящее в том, что студенты со средним и высоким уровнем подготовки мотивированы к процессу генерирования идей с помощью феномен-процедуры «социальное сравнение».

Данная процедура может быть интегрирована в технологию электронный «мозговой штурм» в виде интерактивной таблицы «табель самооценивания», которая ежедневно обновляется преподавателем и имеет открытый доступ для каждого участника команды. Табель содержит информацию о количестве идей, сформулированных каждым студентом. Использование данной таблицы позволяет:

– увеличить мотивацию каждого студента относительно улучшения собственных достижений;

– поместить каждого студента в ситуацию сравнения на базе познания количества идей, сформулированных коллегами;

– упростить оценивание вклада каждого студента в разработку проекта.

После окончания фазы формулирования/генерирования идей, которая может длиться до трех недель, студенты получают доступ к банку идей команды. Студентам предлагается сделать индивидуальную классификацию всех появившихся идей: от самых подходящих идей, которые могут привести к решению задачи, сформулированной в проекте, к менее подходящим идеям. Личная фаза способствует так называемому когнитивному созреванию, которое состоит в интегрировании и ассоциировании различных идей, предложенных коллегами. Созреванию способствует групповая рефлексия (коллективное самопознание). Групповая рефлексия включает в себя критическое осмысление участниками группы результатов своей деятельности, поиск новых путей решения задачи, планирование и анализ совместных действий, приводящих к новому и более глубокому пониманию участниками группы сложившейся ситуации [16].

После фазы личной классификации идей следует фаза коллективной деятельности. Различные персональные классификации обсуждаются и, в результате, составляется коллективная (совместная) классификация идей. На данной фазе мотивации и эффективности обучения способствует наличие социокогнитивного конфликта. Участники команды осознают факт существования решений, отличающихся от тех, что предложены ими самими. Дебаты, которые происходят на данной фазе, обязывают участников искать дополнительную информацию, что приводит их к другому уровню понимания, т.е. к самостоятельному приобретению новых знаний. Дебаты, в свою очередь, способствуют формированию у студентов ряда навыков и качеств:навык слушать/читать и понимать точку зрения другой личности;навык сжатого формулирования идей и мыслей; навык анализа идеи, поиска ее сильных и слабых сторон; навык формулирования аргументов «за» и «против» относительно идеи, точки зрения; проявление терпимости к другим точкам зрения и идеям; развитие критического мышления. После выполнения совместной классификации идей и выбора наилучшего решения, команда начинает реализацию проекта. Как правило, на протяжении данной фазы студенты выполняют различные роли: дизайнера, редактора, аниматора, координатора и др.

III этап – оценивание (последние 2 недели обучения) разбит на две фазы: 1) обсуждение реализованного продукта совместно с преподавателем. Данная фаза может быть осуществлена как в сети, так и очно; 2) защита проекта командой в присутствии академической группы, которая осуществляется в очном режиме.

В ходе эксперимента учебные блоги использовались в качестве:

– индивидуального рабочего инструмента (как для преподавателя, так и для студентов);

– рабочего инструмента (для студентов), содержащего заметки по посещаемым дисциплинам, список полезных веб-адресов.

– рабочего инструмента (для преподавателей), с помощью которого преподаватели публикуют (в открытом или закрытом виде) заметки о преподаваемых дисциплинах, научных статьях, встречах научного характера, новых идеях, появляющихся в области их специализации и др.

– рабочего инструмента по дисциплине, используемого преподавателем в качестве среды преподавания и обучения студентов, в которой опубликовались новости о преподаваемых дисциплинах, ссылки на дидактические материалы, комментарии студентов (для обратной связи);

– рабочего инструмента в группе, используемого студентами для работы над проектом.

Эксперимент показал, что применение образовательного сетевого сообщества в методике обучения информатике позволяет уменьшить негативное воздействие и риски современной информационно-образовательной среды вузов [17], а также оптимизировать ряд организационных форм взаимодействия между студентами и преподавателями [18]:

– студенты и преподаватели, которые не имеют персональных сайтов или не являются участниками социальных сетей, могут общаться друг с другом с помощью блога;

– студенты внимательнее редактируют собственные комментарии, осознавая, что они будут прочитаны другими людьми;

– студенты могут дискутировать с коллегами о деталях, относящихся к проведению дисциплины;

– студенты могут использовать ссылки учебного блога для консультации с другими источниками информации, относящимися к содержанию дисциплины;

– студенты могут общаться с преподавателями, которые ведут лекционные, семинарские и лабораторные занятия;

– преподаватели могут предоставить дополнительную информацию по организации самостоятельной работы студентов;

– студенты получают возможность сотрудничать и взаимодействовать с более широким окружением студентов и преподавателей;

– преподаватели могут наблюдать и оценивать деятельность студентов во время проведения занятий и самостоятельной работы вне занятий.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамян Г.В., Катасонова Г.Р. Таксономия, классификация и методология анализа целей обучения информатике и информационным технологиям в условиях глобализации образования // Фундаментальные исследования, 2014, №8–7, С.1647–1652.
2. Фокин Р.Р., Абрамян Г.В. Метамодель обучения информационным технологиям в высшей школе. – СПб.: Изд-во СПбГУСЭ, 2011, 211с.
3. Абрамян Г.В. Телекоммуникационные модели образования и научной деятельности как облачные сервисы SAAS/SOD взаимодействия в вузе // Перспективы развития науки и образования: сборник научных трудов по материалам Международной научно-практической конференции: в 7 частях, 2013, С.100–101.
4. Аржанов И.Н. Методика обучения объектно-ориентированному проектированию студентов педагогических вузов: автореф. дис. канд. пед. наук: 13.00.02. – СПб., 2000, 18с.
5. Сергеев А.Н. Подготовка будущих учителей информатики к профессиональной деятельности в сетевых сообществах Интернета: автореф. дисс. д. пед. наук: 13.00.02. – СПБ., 2010, 39с.
6. Сысоев П.В. Блог-технология в обучении иностранному языку // Язык и культура, 2012, №4 (20), С.115–127.
7. Рыбалко Т.Г. Использование социальных сервисов Веб 2.0. в профессиональном лингвообразовании // Стендовый доклад. Всероссийская научно-практическая конференция «Электронная Казань» (27–29 апреля 2009). [Электронный ресурс]. – URL: http://www.ksu.ru/conf/ek2009/sbornik/95.doc
8. Абрамян Г.В. Организация средств обратной связи на основе использования глобальных компьютерных телекоммуникационных инфраструктур в регионе // Информатика – современное состояние и перспективы развития. 51 Герценовские чтения: тезисы докладов. – СПб.: Изд-во РГПУ им. А.И. Герцена, 1998, С.22–23.
9. Фролов И. Блог в помощь или Блогосфера как информационная составляющая образовательного пространства региона // Учительская газета. – 9 декабря 2008 г. [Электронный ресурс]. – URL: http://www.ug.ru/archive/26837
10. Иванченко Д.А. Перспективы применения блог-технологий в Интернет-обучении // Информатика и образование, 2007, №2, С.120–122.
11. Лазуткина Е.В. Использование блогов в формировании информационной культуры студентов // Открытое и дистанционное образование, 2010, №1, С.68–73.
12. Сергеев А.Н. Сетевое сообщество как субъект образовательной деятельности в Интернет // Современные проблемы науки и образования, 2012, №6. – URL: http://www.science-education.ru/106-7475
13. Абрамян Г.В. Технологии дистанционного обучения с использованием телекоммуникаций // Информатика - исследования и инновации: межвузовский сборник научных трудов. – СПб.: Изд-во РГПУ им. А.И. Герцена, 1998, С.91–95.
14. Абрамян Г.В. Дистанционные технологии в образовании // Г.В. Абрамян. – СПб.: Изд-во ЛГОУ им. А.С. Пушкина, 2000, 184с.
15. Моглан Д.В. Познавательная деятельность студентов с образовательном сетевом сообществе // Вестник КГПУ им. В.П. Астафьева, 2014, №4 (30), С.67–70.
16. Журавлев А.Л., Нестик Т.А. Групповая рефлексивность: основные подходы и перспективы исследований // Знание. Понимание. Умение, 2011, №3, С.212–221.
17. Абрамян Г.В. Системы и технологии электронного обучения как потенциальные объекты риска информационно-образовательной среды вузов и школ российской федерации // Электронное обучение в вузе и школе: материалы сетевой Международной научно-практической конференции. – СПб.: Изд-во РГПУ им. А.И. Герцена, 2014, С.17–20.
18. Моглан Д.В. Типы взаимодействий в образовательном сетевом сообществе // Вестник СамГТУ. Сер. Психолого-педагогические науки, 2014, №3 (23), С.145–151.

УДК 004.91, 378.146

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО БОРЬБЫ С ПАРАЛЛЕЛЬНЫМ РЫНКОМ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ

Степанов Александр Георгиевич, Космачев Валентин Михайлович,
Шкиртиль Марина Ароновна
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д.67
e-mails: georgich_spb@mail.ru, kvm@aanet.ru, mshkirtil@gmail.com

Аннотация: Требования нового стандарта образования ФГОС ВО+ заставят вузы использовать системы управления учебным процессом для хранения результатов творческой деятельности студентов с целью последующего оценивания их компетенций. В условиях существования предложения на изготовление любых аттестационных заданий на параллельном рынке образовательных услуг возникает необходимость контроля авторства представленных материалов. Предлагается организовать борьбу с указанным явлением за счет создания портфолио выпускника, которое собирает вуз за время его обучения и хранит все время его активной профессиональной деятельности.

Ключевые слова*: студенческий плагиат; высшее образование; параллельный рынок образовательных услуг; торговля контрольными заданиями; портфолио*

INFORMATION TECHNOLOGY AS A MEANS OF STRUGGLE WITH PARALLEL THE EDUCATION MARKET

Aleksandr Stepanov, Valentin Kosmachev, Marina Shkirtil
The St. Petersburg State University of aerospace instrumentation,
Russia, St. Petersburg, Bolshaya Morskaia str. 67,
e-mails: georgich_spb@mail.ru, kvm@aanet.ru, mshkirtil@gmail.com

Abstract: Requirements of the new standard will make education colleges use learning management system to store the results of creative activity of students for subsequent evaluation of its competences. Under the conditions of the existence of offers on the parallel market of educational services for the manufacture of any certification tasks it is necessary to control the authorship of the submissions. It is proposed to organize the struggle with this phenomenon by creating a portfolio of graduates who collects during his high school education and stores all the time of his active professional work

Keywords*: students' plagiarism; higher education; parallel market for educational services; tests for sale; portfolio*

Начиная с сентября 2014 года в практику работы высшей школы внедряются новые стандарты высшего образования ФГОС ВО+. Основным их отличием от предыдущих вариантов является требование обязательного формирования у студентов в процессе обучения набора компетенций, под которыми понимается способность и готовность выпускников применять знания, умения и навыки, успешно действовать на основе практического опыта при решении широкого круга задач (в том числе в профессиональной деятельности) [1]. В то же время впервые требования к самим знаниям, умениям, навыкам и владениям выпускников в самих стандартах не формулируются, что позволяет высшим учебным заведениям самостоятельно разрабатывать всю технологию обучения конкретному направлению или специальности.

Оценка результатов подготовки в целом с позиции именно сформированности компетенций выпускника невозможна без анализа и качественной оценки промежуточных результатов обучения. При использовании предыдущих вариантов стандартов такими промежуточными результатами как раз и были знания, умения и навыки, которые проверялись в процессе тестирования, сдачи зачетов и экзаменов и соответствующим образом оценивались. Теперь контроль формирования компетенций обучаемого придется проводить уже на основе анализа результатов его творческой индивидуальной деятельности. Они формализуются в виде отчетов по лабораторным работам, рефератов, домашних заданий и контрольных работ, отчетов по практикам, пояснительных записок к курсовым и выпускным квалификационным работам, а также в виде результатов научной деятельности (докладов, статей, отчетов по НИР и т.д.). Все эти материалы в процессе обучения проверяются (оцениваются) преподавателями, выступающими в роли экспертов.

Дополнительный контроль сформированности компетенций выпускника может проводится во время проведения государственной аккредитации высшего учебного заведения. Традиционная для таких случаев процедура контроля знаний и умений студентов становится невозможной в силу отсутствия общих для всех вузов требований в этой области. Поэтому практиковавшееся ранее при

аттестации тестирование остаточных знаний станет невозможным и проверяющим придется сосредоточиться, например, на изучении курсовых и выпускных работ.

Непрерывная модернизация российского образования происходит, кроме всего прочего, в условиях существования параллельного рынка образовательных услуг. Он предлагает выполнение продавцом-исполнителем аттестационных заданий покупателя-заказчика. Подобного рода услуги оказываются всем желающим и свободно рекламируются самыми разными способами. Размер рынка весьма велик, а предложение и спрос охватывают все составляющие начиная с контрольных работ заочников и заканчивая докторскими диссертациями [2]. Очевидно, что приобретение услуги на таком рынке с последующей сдачей аттестационного задания является мошенничеством. Исследователи проблемы отмечают существование по крайней мере двух составляющих такого мошенничества: плагиата и факта «несамостоятельности при написании работы» [3].

Проведенные опросы свидетельствуют, что 91% студентов признает, что они прибегали к недобросовестному заимствованию при подготовке к сдаче студенческих работ, используя бесплатные работы из интернета, а 7% заказывали свои работы за деньги [4]. Схожие по смыслу результаты опросов американских исследователей приведены и в работе [3]. Приходится признать, что платная образовательная услуга параллельного рынка свободно оказывается всем желающим, а само существование такого рынка обесценивает систему высшего образования, что вступает в противоречие с интересами общества.

Причин широкого распространения различных форм плагиата несколько. Однако в основе лежит желание получить преимущество над конкурентами в кадровом отборе [2]. В сознании определенной и достаточно большой группы граждан качество образования ассоциируется не с уровнем профессиональной подготовки, а с престижностью «корочек». Многие люди рассматривают поступление в вуз как возможность получения некого квалификационного свидетельства, а не как средство собственного развития и удовлетворения интереса к знаниям. Поэтому они обращаются к тем, кто может помочь им достигнуть своей цели без особых усилий. Высокое качество услуг продавцов параллельного рынка при попустительстве преподавателей вузов трансформируется в высокие оценки вкладыша в диплом и не соответствующий им уровень профессиональной подготовки выпускника, искажающий оценку прочими потребителями (в частности, работодателями) реальных образовательных услуг, оказываемых учебными заведениями [5].

В обществе возникают самые разнообразные идеи борьбы с описываемым явлением. Г.Ф. Хасанова [4] отмечает необходимость оказания большего внимания вопросам инженерной этики. Тем не менее, большинство предлагаемых методов сводится скорее к контрольно-запретительным действиям, чем к системной борьбе с обсуждаемым опасным для общества явлением. Так большое внимание уделяется разработке документации, регламентирующей проведение учебного процесса. Формализуются процедуры сдачи экзаменов (в том числе и вступительных), защит квалификационных работ и диссертаций. Появляются дополнительные требования в части документальной поддержки процесса аттестации, включающие в себя в том числе и средства видео фиксации. Ужесточаются кадровые требования к привлекаемым к аттестации специалистам. Ну и, конечно, увеличивается общий объем подготавливаемой и хранимой в бумажном виде документации.

К числу предложений по противодействию плагиату можно отнести выдвинутую на самом высоком уровне мысль о тотальной проверке всех студенческих работ соответствующими программными средствами. Являясь по сути правильным, это предложение, к сожалению, крайне затруднительно в реализации из-за большого объема затрат на его воплощение в жизнь. Несмотря на наличие различных систем автоматизированной проверки на неправомерные заимствования [6], реализовать тотальную проверку всего необходимого материала не удается даже на уровне докторских диссертаций. Поэтому рассчитывать на то, что, кроме всего прочего, вузы будут проверять все оцениваемые студенческие материалы в срок и в полном объеме не приходится хотя бы потому, что преподаватели до сих пор не понимают, что собственно нужно им делать в случае выявления факта плагиата. Оценить положительный эффект от перечисленных действий представляется затруднительным, как, впрочем, и необходимый объем затрат.

При разумной организации учебного процесса все результаты деятельности студента сохраняются в системе управления обучением. Уже сейчас такие системы обеспечивают существенно новые возможности реализации учебного процесса, что, в конечном итоге, оказывает положительное влияние на результаты обучения в целом [7]. Логично предположить, что в процессе внедрения стандартов ФГОС ВО+ роль таких систем будет только возрастать. Выполняя свою основную функцию, системы управления обучением сохраняют в цифровом виде весь объем отчетного материала за все 10 лет обучения в вузе [8]. Конечно, эта информация будет играть большую роль в процессе обучения при аттестации студента и при аккредитации и лицензировании самого вуза.

Еще больший интерес курсовые и выпускные работы будет представлять для потенциальных работодателей. Как бы точно ни были бы сформулированы компетенции и как бы качественно ни

была бы организована проверка на их соответствие, требования конкретных рабочих мест отличаются и будут отличаться.

Рис.1. Составляющие портфолио выпускника в части оцениваемых результатов обучения

В процессе своей профессиональной жизни выпускник будет неоднократно проходить процедуру собеседования на предмет назначения на очередную должность. Уже сложилась практика обязательного предоставления работодателю резюме соискателя должности. Вполне логично было бы предположить, что в некоторых случаях претендент на должность должен был бы предоставлять и информацию о своих профессиональных достижениях за все время его деятельности, которую иногда называют портфолио [9]. В его состав как раз и могли бы быть включены хранящиеся в архиве системы управления обучением тексты выполненных за время обучения курсовых и итоговых работ, отчеты по практикам, а также результаты их оценивания (рис.1).

В этом случае проверка компетенций студента будет носить адресный характер, в чем заинтересовано большинство нормально обучающихся людей, и будет проводиться тогда, когда в ней возникнет необходимость, например, при поступлении на высокооплачиваемую работу, а не в момент аттестации или защиты.

Высшие учебные заведения заинтересованы в отслеживании судьбы своих выпускников. Поэтому они с удовольствием займутся ведением их портфолио в электронном виде. Потребуется разработать процедуру доступа к этим данным учитывая, в том числе, и требования информационной безопасности. Тогда все участники образовательного процесса будут знать, что существует, пускай и не очень большая, вероятность того, что текст курсовой или квалификационной работы может быть проверен работодателем на плагиат через много лет после защиты диплома или диссертации. Факт его обнаружения может стоить претенденту должности. Это обстоятельство будет отрезвляюще действовать на желающих участвовать мошенничестве. Попытка обучения по коррупционным схемам станет опасной для потребителя продукции параллельного рынка. Как следствие, студент будет осознавать, что его подлог (если он был) зафиксирован и может вскрыться в любой момент его профессиональной жизни, что, в конечном итоге, должно оздоровить существующую ситуацию в образовании.

СПИСОК ЛИТЕРАТУРЫ

1. Анисимова М. А. К вопросу о проектировании оценочных средств сформированности компетенций / М. А. Анисимова, И. С. Бляхеров, А. В. Масленников, А. В. Моржов // Высшее образование в России. 2013. № 4. С. 106-113.
2. Абрамов А. М. Плата плагиата / А. М. Абрамов // Аккредитация в образовании. 2013. № 2 (62). С. 80-82.
3. Кичерова М. Н. Плагиат в студенческих работах: анализ сущности проблемы / М. Н. Кичерова, Д.Н. Кыров, П.Н. Смыкова, С.А. Пилипушко // Интернет-журнал Науковедение. 2013. № 4 (17). С. 82.
4. Хасанова Г. Ф. Об этических представлениях студентов полимерных специальностей / Г. Ф. Хасанова // Вестник Казанского технологического университета. 2013. т. 16. № 6. С. 331-333.
5. Миляева Л. Г. Параллельный рынок услуг высшего профессионального образования (торговля контрольными заданиями) / Л. Г. Миляева, О. В. Борисова // Terra Economicus. 2010. Т. 8. № 3. С. 122-133.
6. Чиркин Е. С. Системы автоматизированной проверки на неправомерные заимствования / Е. С. Чиркин // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2013. № 12 (128). С. 164-174.
7. Информационные технологии в работе кафедры / А. Н. Бабенков, В. С. Блюм, С. Д. Бодрунов и др. // под общ. ред. А.Г. Степанова. – СПб.: ГУАП, 2014, 276 с.
8. Флегонтов А. В. 10=4+2+4 / А. В. Флегонтов // Информационные системы и технологии. Межвузовский сборник научно-технических статей. 2014. № 3. С. 17-20.
9. Минобрнауки планирует ввести портфолио для молодых учителей. ТАСС Информационное агентство России. 05.11.2014. [В Интернете]. URL: http://itar-tass.com/obschestvo/1551611. [Дата обращения: 09.12.2014].

УДК 378.14.015.62

СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБУЧЕНИИ БУДУЩИХ ЭКОНОМИСТОВ

Степанов Александр Георгиевич, Карасева Екатерина Ивановна, Зуева Наталья Васильевна, Москалева Ольга Ильинична,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д. 67,
e-mails: georgich_spb@mail.ru, matatka@hotbox.ru, n_v_zueva@mail.ru, o.i.moskaleva@gmail.com

Аннотация: На основании анализа требований профессиональной компетенции рассмотрено обучения вопросам информационной безопасности при подготовке по экономическим направлениям.

Ключевые слова*: информационная безопасность, высшее профессиональное образование, компетентностная модель, структура содержания обучения*

COMPONENTS OF INFORMATION SECURITY TRAINING IN FUTURE ECONOMISTS

Stepanov Alexander, Karaseva Ekaterina, Zueva Natalia, Moskaleva Olga,
Saint-Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaia str. 69,
e-mails: georgich_spb@mail.ru, matatka@hotbox.ru, n_v_zueva@mail.ru, o.i.moskaleva@gmail.com

Abstract: *Based on the analysis requirements of professional competence is developed training content information security issues in preparation for economic fronts.*

Keywords*: information security, higher vocational education, competence model, the structure of teaching content*

Маловероятно, что кто-то сомневается в необходимости овладения знаниями, умениями и навыками в области информационной безопасности выпускниками высшей школы. В работе В.П. Полякова [1, с.39] выделяется несколько групп категорий выпускников вузов, которым необходима соответствующая подготовка. К последней четвертой группе можно отнести практически всех выпускников, для которых информационная подготовка является базовой. Очевидно, что к этой же категории можно отнести и выпускников укрупненной группы направлений 38.00.00 Экономика и управление. Хотя новая система образовательных стандартов ФГОС ВО уже введена в практику высшей школы, на сегодняшний день утверждены только стандарты обучения в магистратуре, а стандарты специалитета и бакалавриата рассматриваемой укрупненной группы все еще находятся в стадии утверждения и существуют только в виде проектов.

Основное отличие обсуждаемых стандартов от используемых ранее заключается в повсеместном внедрении так называемого компетентностного подхода. Фактически новые стандарты отказываются от традиционного регламентирования знаний, умений и навыков выпускников и сосредотачиваются на требованиях к результатам подготовки в аспекте овладения выпускниками именно компетенциями. Одно из определений этого понятия содержится, например, в работе М.А. Анисимовой [2, с.107] «компетенция – это способность и готовность применять знания, умения и навыки, успешно действовать на основе практического опыта при решении широкого круга задач (в том числе в профессиональной деятельности». Очевидно, что перечень необходимых знаний, умений и навыков в этом случае определяется уже составителями образовательных программ подготовки. Внедрение новых стандартов приводит к существенному изменению процедуры составления учебного плана и системы организации учебного процесса. Отметим, что впервые учебный план может формироваться исходя из возможностей конкретного высшего учебного заведения и нацеливаться не на промежуточные, а на итоговые результаты обучения.

Вопросы информационной безопасности изучаются еще в средней школе. Как отмечают И.В. Симонова и М.И. Бочаров [3], несмотря на то, что в стандартах средней школы явно указано понятие информационная безопасность, основное внимание школьников концентрируется на вопросе защиты информации. А если в действующих учебниках и приводится понятие информационной безопасности, то оно трактуется, как правило, в узком смысле. Проведенный в работе [3] анализ показывает, что требования стандарта реализуются в средней школе не в полной мере и, как следствие, преподавателям высшей школы приходится рассчитывать на определенный уровень начальной подготовки в области информационной безопасности.

Анализ компетенций, сформулированных в уже утвержденных стандартах подготовки магистров укрупненной группы направлений подготовки 38.00.00 Экономика и управление показал, что разработчики стандартов не предусматривают отдельных компетенций выпускников, связанных с вопросами информационной безопасности. Таким образом, можно сделать вывод, что разработчики стандартов магистратуры предполагают, что необходимые компетенции уже сформированы в

процессе обучения в бакалавриате.

Анализ проектов стандартов подготовки бакалавров и специалистов показал, что большинство из них (Экономика, Менеджмент, Управление персоналом, Государственное и муниципальное управление, Торговое дело) предусматривают только одну компетенцию выпускников, связанную с информационной безопасностью: «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности». Эту же компетенцию должны обеспечивать выпускники направления Бизнес-информатика, однако к ней добавляются еще компетенции: «организация взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия», «умение защищать права на интеллектуальную собственность», «умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия». Стандарт специальности Таможенное дело также предусматривает общую для всех выше упомянутых направлений подготовки компетенцию и добавляет еще: «умением обеспечивать в пределах своей компетенции защиту прав интеллектуальной собственности». Ну и по направлению Товароведение и специальности Экономическая безопасность отдельных компетенций в области информационной безопасности нет.

Экономическая подготовка в университетах осуществляется, как правило, по нескольким или даже по всем направлениям или специальностям, предусмотренным стандартами образования. Из соображений экономии своих средств вузы стремятся, насколько это возможно, ее унифицировать. Касаясь рассматриваемого вопроса и учитывая в основном одинаковые требования компетенций выпускников подобные действия представляются оправданными. Очевидно, что имеет смысл говорить о разделе традиционно изучаемой дисциплины Информатика или даже о самостоятельной дисциплине Информационная безопасность. Представляется обязательным дать студентам общую структуру теории информационной безопасности, поскольку только в этом случае можно обеспечить фундаментальность подготовки.

В соответствии с Научно-методологическими основами информатизации Р.М. Юсупову и В.П. Заболотскому [4], выделим основные составляющие информационной безопасности (рис. 1).

Рис. 1. Составляющие информационной безопасности

Экономическую безопасность в аспекте рассматриваемого вопроса обеспечивают информационные ресурсы. Под ними в первую очередь понимается интеллектуальный продукт деятельности квалифицированной и творчески активной части населения страны. Еще одна составляющая экономической безопасности – это информационное пространство, на основе которого сейчас формируется информационное общество, в котором «производство и потребление информации является важнейшим видом деятельности, информация признается наиболее значимым стратегическим ресурсом, … информационные технологии … становятся базовыми технологиями, а основу инфраструктуры общества формирует информационно-коммуникационная инфраструктура» [5, с. 40]. Ну и в качестве самостоятельного вопроса отметим оценку рисков, связанных с нарушением информационной безопасности, а также оценку затрат на ее реализацию [6], [7], [8].

Оборонную безопасность применительно к рассматриваемой тематике целесообразно рассматривать в отношении информационного оружия и информационных войн. «Информационное оружие – это совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию; ограничивать или прекращать доступ к ней законных пользователей; нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства. А также информационное оружие способно меняет сознание людей, заставляет их неадекватно воспринимать реальность, жить в мире иллюзий и совершать гибельные для себя поступки [9] с.403. Информационная война затрагивает все составляющие функционирования информационного общества, обычно не объявляется, представляет собой существенную угрозу и уже ведется (см., например, [10]). Важным самостоятельным вопросом, связанным с оборонной безопасностью, является использование информационных технологий для борьбы с терроризмом [11].

Социальная информационная безопасность может рассматриваться применительно к специфике социального управления [12], противодействия социальным отклонениям [13], угрозам для

и от виртуальных сообществ в социальных сетях [14], [15], интернет-зависимости [16], психологической устойчивости [17], образованию [18] и противодействию экстремизму [19]. Сюда же относятся вопросы, связанные с интеллектуальной собственностью [20].

Экологическая безопасность связана с информационной через проблемы передачи обществу необходимой сведений о различного рода угрозах, например, в случае природных и техногенных катастроф. Существование развитого информационного пространства (средства массовой информации, интернета и социальных сетей существенно повышают информированность граждан, однако в целом подобная информация не доходит до всех заинтересованных адресатов или существенно опаздывает, хотя в стране и существует общероссийская комплексная система информирования и оповещения населения [21], [22]. Еще один аспект экологической безопасности – улучшение с существующих технологий, которое возможно за счет внедрения информационных технологий во все сферы экономики. В этом случае возможно внедрение «экологически чистых», энерго и ресурсосберегающих, безотходных технологий [4]. Некоторые примеры постановки и решения обсуждаемых вопросов описаны в [23], [24], [25], [26].

Проведем синтез содержания обучения вопросам информационной безопасности для современной высшей экономической школы и воспользуемся для этого ранее разработанными методиками [27], [28]. В качестве исходного уровня подготовки будем предполагать, что выпускники средней школы освоили технические средства защиты информации, организационные аспекты информационной безопасности человека как на индивидуальном уровне, так и на уровне государства, знакомы с понятиями информационной этики (этика интернета, компьютерная этика, сетевой этикет, этика сетевого общения, нормы поведения в сети, этические нормы, этические нормы информационной деятельности, этичное поведение при использовании информации) [29]. Приведенные в работе [30] результаты анализа учебников для средней школы показывает, что при успешном освоении учебного материала такое предположение вполне обосновано. Поэтому можно предположить, что выпускники будут обладать достаточными компетенциями в вопросах социальной информационной безопасности за исключением вопросов, связанных с интеллектуальной собственностью.

Экономическая безопасность при подготовке основных направлений экономического бакалавриата становится важнейшей составляющей профессиональных компетенций выпускников в рассматриваемой области. Основным вопросом в этой области становится безопасность информационных технологий. Воспользовавшись результатами [27] и учитывая соображения, связанные с оборонной и экологической безопасностями, сформулируем содержание результатов обучения как понимание сущности и понятия информационной безопасности, ее составляющих, а также места информационной безопасности в системе национальной безопасности. Также необходимо обеспечить компетенции в области защиты информации и информационных технологий, а также существующей законодательной базы в том числе и в области интеллектуальной собственности. Скорее всего имеет смысл внести эти вопросы в структуру базового курса Информатики. Аналогичная ситуация складывается и при подготовке специалистов в области экономики.

Подготовка по направлению Бизнес-информатика требует более глубоко освоения материала. Поэтому предлагается выделить самостоятельную дисциплину Информационная безопасность с систематическим изложением всех составляющих информационной безопасности, а в дисциплине Информатика уделить большее внимание вопросам социальной безопасности с целью совершенствования компетенций, освоенных в средней школе.

Очевидно, что высказанные соображения представляют собой точку зрения авторов работы. Считаем целесообразным обсудить их во время проведения конференции, затронув дополнительно вопрос о структуре подготовки по вопросам информационной безопасности для профильных в области информатики направлений и специальностей высшей школы.

СПИСОК ЛИТЕРАТУРЫ

1. Поляков В.П. Аспекты информационной безопасности информационной подготовки в системе высшего профессионального образования / Глобальный научный потенциал. 2012. №13. С. 39–43.
2. Анисимова Т.И. Организация самостоятельной работы бакалавров средствами дистанционного обучения / Фундаментальные исследования 2013. №11-4. С. 747–750.
3. Симонова И.В., Бочаров М.И Анализ содержания обучения школьников в области информационной безопасности / Информатизация образования и науки. 2014. №2 (22). С. 61–79.
4. Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. СПб.: Наука. 2000, 455 с.
5. Юсупов Р.М. Информационные технологии и экономика информационного общества / Инновации. 2013. №11 (181). С. 40–46.
6. Зегжда П.Д. Обеспечение безопасности информации в условиях создания единого информационного пространства / Защита информации. Инсайд. 2007. №4 (16). С. 28–33.
7. Петренко С.А., Обухов, А.В. Антикризисные политики информационной безопасности / Защита информации. Инсайд. 2009. №2 (26). С. 59–61.
8. Петренко С.А., Обухов, А. В. Антикризисные политики информационной безопасности / Защита информации. Инсайд. 2009. №3 (27). С. 74–78.
9. Андрусова Т.Б. Гомонова Ю.Г., Багаева А.П. Информационное оружие и информационные войны / Актуальные проблемы авиации и космонавтики. 2010. Т. 1, №6. С. 403–404.

10. Морозов А.В., Майбуров Д.Г., Чукляев И.И. Информационное оружие: теория и практика применения / Проблемы безопасности Российского общества 2014. №2. С. 177–183.
11. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом / Защита информации. Инсайд. 2009. №2 (26). С. 74–79.
12. Захаров М.Ю. Информационная безопасность – основополагающий элемент безопасности социального управления / Вестник университета (Государственный университет управления). 2012. №9-1. С. 112–115.
13. Демчук С.Д. Информационная безопасность как один из аспектов противодействия социальным отклонениям / Информационная безопасность регионов. 2013. №1 (12). С. 21–27.
14. Прончев Г.Б., Монахов Д.Н., Ланцов В.В. Безопасность виртуальных социальных сред в информационном обществе / Пространство и время. 2013. №4 (14). С. 231–236.
15. Акаев В.Х., Шамсуев М.-Х. Безопасность юга России: информационные угрозы социальных сетей / Вестник академии наук Чеченской республики. 2011. №2 (15). С. 156–158.
16. Завалишина О.В., Загуменных Н.А., Постоева Е.С. Интернет-аддикция - одна из актуальных проблем современности / Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. №105. С. 226–235.
17. Лунев А.Н., Н.Б. Пугачева, Стуколова Л.З. Информационно-психологическая безопасность личности: сущностная характеристика / Современные проблемы науки и образования. 2014. №1. С. 21–32.
18. Карабанов С. Н. Информационная безопасность и социально-гуманитарный компонент профессионального образования / Актуальные проблемы гуманитарных и естественных наук. 2014. №12-2. С. 262–264.
19. Мозговой В.Э. Особенности информационной экстремистской деятельности: социологический анализ / Вестник Костромского государственного университета им. Н.А. Некрасова. 2014. Т. 20. №7. С.220–224.
20. Рудь С.Н. Применение информационных технологий в защите объектов интеллектуальной собственности / Логистические системы в глобальной экономике. 2014. №4. С. 441-443.
21. Рыженко А.А. Рыженко Н.Ю., Эльтемерова О.В. Проблемы информирования и оповещения населения о чрезвычайных ситуациях / Технологии техносферной безопасности. 2014. №2 (54). С.24.
22. Демченко О.Ю., Удилова И.Я., Шевцов С.А. Психологические особенности информирования населения в условиях чрезвычайной ситуации / Вестник Воронежского института ГПС МЧС России. 2014. №1 (10). С.32–35.
23. Каган П.Б., Хоркина Ж.А., Зуева А.В. Мониторинг градостроительного развития городских территорий, в том числе с использованием информационных технологий / Инженерно-строительный журнал. 2012. № 9 (35). С. 3–8.
24. Шедий Е.Г. Новые информационные технологии на службе у агрохолдинга / Российское предпринимательство. 2010. №12-2. С.136-141.
25. Шевченко И.Ю. Инновационное развитие промышленного нефтехимического производства с использованием информационных технологий и моделирования / Вестник Алтайской академии экономики и права. 2014. № 5 (37). С. 65-67.
26. Романов Ю.А. Интеллектуальная собственность как социально-экономический ресурс общества / Социология власти. 2009. №1. С.24-25.
27. Макарова Н.В., Степанов А.Г. Информатика в системе непрерывного образования. Монография. СПб.: Политехника. 2005. 338 с.
28. Степанов А.Г. Объектно-ориентированный подход к отбору содержания обучения информатике. СПб.: Политехника. 2005.
29. Бочаров М.И., Симонова И. В. Методика обучения информационной безопасности старшеклассников / Пространство и время. 2013. №4 (14). С. 237-244.
30. Бочаров М.И., Симонова И.В. Методика обучения информационной безопасности старшеклассников: о содержании обучения информационной безопасности в школьном курсе информатики / Пространство и время 2014. №3. С. 300-307.

УДК 004.91, 378.146

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ПОВЫШЕНИИ КАЧЕСТВА ОЦЕНКИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

Степанов Александр Георгиевич, Семенова Елена Георгиевна, Фролова Елена Александровна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д.67,
e-mails: georgich_spb@mail.ru, egsemenova@mail.ru, frolovaelena@mail.ru

Аннотация: Проводится сопоставление характеристик выпускных квалификационных работ бакалавров, специалистов, диссертаций магистров и диссертаций на соискание ученых степеней кандидатов и докторов наук, а также сравнение параметров (критериев) их оценки. Показано, что в связи с введением нового поколения стандартов, нацеленного на обеспечение компетентностей выпускников, существующая система оценивания результатов обучения требует существенной переработки.

Ключевые слова: *итоговая государственная аттестация; Федеральный государственный образовательный стандарт, компетенции; выпускная квалификационная работа; компетентностный подход.*

INFORMATION TECHNOLOGY TO IMPROVE THE QUALITY OF EVALUATIONQUALIFYING WORK STUDENTS

Aleksandr Stepanov, Elena Semenova, Elena Frolova,
The St. Petersburg State University of aerospace instrumentation,
Russia, St. Petersburg, Bolshaya Morskaia str. 67,
e-mails: georgich_spb@mail.ru, egsemenova@mail.ru, frolovaelena@mail.ru

Abstract: A comparison of the characteristics of the final qualifying works of bachelors, specialists and master's theses and dissertations for academic degrees and Ph.D., as well as a comparison of parameters (criteria) of their assessment. It is shown that due to the introduction of a new generation of standards aimed at ensuring the competence of graduates, the current system of assessment of learning outcomes requires substantial processing.

Keywords: *final state certification; federal state educational standard, competence final qualifying work; competence-based approach*

Важнейшими задачами высших учебных заведений является достижение системой образования следующих целей обучения:

удовлетворение потребности человека в образовании;

становление и развитие творческой личности;

подготовка выпускников, обладающих необходимыми компетенциями, теоретическими знаниями и практическими навыками по направлениям профессиональной деятельности;

присуждение успешным выпускникам квалификации в виде ученых степеней (бакалавр, магистр, кандидат наук, доктор наук).

Система образования должна гибко и адекватно реагировать на требования рынка труда и динамику его изменения [1]. Студент получает образование первого уровня (бакалавриат), возможность подготовиться к конкретной профессиональной деятельности на более высоком уровне (магистратура) и далее продолжать обучение в аспирантуре. Общее время, необходимое для получения высшей квалификации без учета докторской степени становится равным 10 годам [2]. Завершая образование на каждом из перечисленных выше уровней обучающийся проходит обязательную процедуру итоговой аттестации. Традиционно в ее содержание включается две формы испытаний – государственный экзамен и защита выпускной квалификационной работы (диссертации). Требования к содержанию, объему и структуре выпускной квалификационной работы в соответствии с Федеральными государственными образовательными стандартами вырабатываются высшими учебными заведениями, осуществляющими обучение по соответствующей образовательной программе. Требования к кандидатским и докторским диссертациям дополнительно регламентируются Высшей аттестационной комиссии (ВАК). Отсюда вытекает необходимость разработки по каждому уровню подготовки требований к выпускным квалификационным работам и организации их защиты.

Итоговая аттестация должна предусматривать конкретный набор минимальных требований к выпускным работам на каждом уровне подготовки. В таблице 1 *Таблица 1*приведен вариант таких требований.

Таблица 1

Сравнение оцениваемых параметров квалификационных работ

Параметр	**Выпускная квалификационная работа бакалавра**	**Диплом (работа/проект) специалиста**	**Магистерская диссертация**	**Кандидатская диссертация**	**Докторская диссертация**
Тема соответствует	направлению	специальности	направлению	специальности диссертационного совета	
Утверждает тему	ректор			ученый совет	
Разрешение проблемы обеспечивает получение эффекта	конкретным объектом исследования	несколькими объектами		отраслью знаний, хозяйства, техники, технологии, культуры, политики. педагогики, экономики и т.п.	страной
Объект исследования	предприятие, учреждение, процесс	группа предприятий, учреждений, процессов		отрасль	страна
Предмет исследования	главное противоречие, описывающее суть проблемы				
Актуальность темы	по отношению к объекту или предмету исследования	по отношению к группе объектов или предметов исследования		по отношению к отрасли знаний	по отношению к стране

Параметр	Выпускная квалификационная работа бакалавра	Диплом (работа/проект) специалиста	Магистерская диссертация	Кандидатская диссертация	Докторская диссертация
Класс исследований	методологические/ прикладные		теоретические/методологические/прикладные		
Научная новизна темы	может отсутствовать	может отсутствовать	присутствует	обязательна	обязательна
Цели и задачи	главная проблема и подпроблемы в виде отдельных задач, а также специальные задачи		главная проблема и подпроблемы в виде отдельных задач		
Теоретическая основа исследования	знания, полученные в результате изучения учебных дисциплин в соответствии с содержанием обучения		знания, полученные в результате изучения научных дисциплин по профилю разрабатываемой проблемы		
Методологическая основа исследования	учебники, монографии	учебники, монографии, статьи	учебники, монографии, статьи, доклады, отчеты, ранее защищенные диссертации		
Научная новизна исследования	относительная		абсолютная		
Практическая значимость исследования	обязательна		обязательна с возможной доработкой	обязательна с возможной дополнительной разработкой методик	
Личный вклад автора.	Работа выполняется индивидуально автором. Ссылки на чужие материалы, в том числе и на материалы соавторов, должны быть правильно оформлены.				
Публикации по теме работы[5]	не обязательны		не менее двух в любых журналах	не менее 2 (3) в журналах из списка ВАК	не менее 10 (15) в журналах из списка ВАК
Апробация результатов исследования	не обязательна		обязательна		
Положения, выносимые на защиту	не обязательны			обязательны	

По мере роста уровня искомой квалификации процедура защиты и оформления необходимой документации становится все более и более сложной. Кроме обычного протокола заседания, ведутся его стенограмма, аудио и видео запись и трансляция в сети Интернет. Предлагается для повышения качества работы, например, диссертационных советов, увеличить их состав до 30-35 человек [3]. Схожие идеи имеют место и при создании государственных аттестационных и экзаменационных комиссий. Реализация данных предложений, в конечном итоге, повлечет за собой создание в университетах специальных аттестационных департаментов, ответственных за организацию и проведение защит выпускных квалификационных работ всех уровней.

Повышение качества процесса аттестации и сокращение затрат на него можно обеспечить за счет автоматизации процесса аттестации с помощью использования соответствующих информационных технологий [4]. Определим набор информационных технологий, которые могут быть использованы в процессе итоговой аттестации. Это технологии автоматизированного офиса и документооборота, мультимедиа, библиотечного дела, справочного и информационного обеспечения [5]. Все перечисленные технологии достаточно распространены и входят в инструментарий учебных и научных подразделений вузов [6].

Отдельное место занимают технологии проведения видеоконференций, с помощью которых обеспечивается трансляция в сети Интернет и запись заседаний аттестационных комиссий, а также технологии поддержки принятия решения комиссии в процессе заседания. Эти технологии сейчас уже достаточно распространены. Они используются, в том числе, и для проведения аттестаций совместно с системами дистанционного обучения [7]. Программная база видеоконференции может опираться на самые разнообразные комплексы (Adobe Acrobat Connect Pro, Elluminate, Dimdim, Open Meeting, Microsoft Office Live Meeting, Lync и др.) [8]. К сожалению, для обеспечения профессиональной видеотрансляции требуются качественное оборудование и аппаратное обеспечение. В конечном итоге проведение защит будет проходить с режиссерами и операторами в специально оборудованных аудиториях, напоминающих телевизионные студии [9], что станет непосильным для отдельных кафедр и будет обеспечиваться специальными службами вуза.

Еще больше проблем вызывает оценивание соответствия защищаемой работы требованиям к выпускным работам соответствующей ступени. Сама процедура тайного голосования в ученых советах, занимающихся присуждением ученых степеней достаточно описана и формализована. Тем

[5] В скобках указано количество публикаций для защит по гуманитарным дисциплинам

не менее, члены ученого совета, выступая в качестве экспертов, дают только интегральную оценку защиты – да или нет. Предполагается, что эксперт из собственных соображений принимает решение о соответствии или несоответствии защищаемой работы отдельным требованиям ВАК.

Сегодня при защите студенческих работ формализация процедуры защиты менее жесткая и сводится, в конечном итоге, к обсуждению оценок после завершения всех защит. Обычно это обсуждение организует один из руководителей экзаменационной комиссии. Внедрение в практику высшей школы стандартов ФГОС заставит изменить и эту составляющую процедуры защиты. Теперь во время ее проведения комиссия будет обязана проверить все компетенции выпускника [10]. Безусловно, защищаемая работа и доклад ее автора достаточно много говорит специалисту о результатах обучения. Однако, принимая решение о присвоении выпускнику квалификации, комиссия должна оценить все требуемые стандартом компетенции. Например, для направления подготовки 09.04.03 Прикладная информатика таких компетенций тридцать одна (из них три общекультурных и шесть общепрофессиональных). Нет сомнений в том, что при существующей технологии защит оценить владение выпускником всеми требуемыми компетенциями невозможно даже при специальной организации структуры выпускной квалификационной работы.

Процедура защиты предусматривает предварительный анализ содержания работы, а также выступление претендента на квалификацию перед комиссией. Можно говорить, что сама защита сопровождается процедурой экспертного оценивания результатов обучения. Контролируемые экспертами параметры при подготовке защиты должны быть формализованы в анкете эксперта – члена аттестационной комиссии. Кроме этого, должна быть разработана процедура обработки результатов анкетирования. В конечном итоге квалификационной комиссией принимается решение о присвоении или отказе в присвоении искомой квалификации формируемое экспертным методом, а также регламентируемый набор документов, который остается в вузе или пересылается в ВАК.

Возможным выходом из ситуации является учет результатов предварительного оценивания некоторых компетенций выпускника. В отличие от знаний, умений и навыков, компетенции можно проверить только в процессе оценивания результатов творческой деятельности студента. За время обучения студент выполняет ряд заданий, которые требуют от него не просто заучивания и тренировки, но и проявления индивидуальных творческих способностей. К таким заданиям можно отнести рефераты, контрольные работы, отчеты о самостоятельной работе по дисциплине, курсовые работы и отчеты о практиках. При составлении учебного плана необходимо обеспечить, чтобы все контролируемые компетенции выпускника в совокупности учитывались соответствующими заданиями и выпускной квалификационной работой. При сопровождении учебного процесса информационной системой управления обучением все эти материалы, созданные за четыре или шесть лет обучения, хранятся в базах данных совместно с результатами их оценивания преподавателями. Тогда члены аттестационной (экзаменационной) комиссии в процессе защиты выпускной квалификационной работы могут получить доступ и к этим материалам, ознакомиться с ними, учесть ранее сделанные результаты оценивания, а также выполнить свое. Все это требует разработки специализированной информационной технологии поддержки принятия решения эксперта в виде оперативного обеспечения его дополнительными проверяемыми материалами, например, курсовыми работами студента, выполненными за все время его обучения, а также предлагает каждому эксперту индивидуальную анкету для оценивания результата защиты, и обработки результатов анкетирования всех членов комиссии.

При реализации предложенной технологии возникают дополнительные требования к оборудованию помещения, в котором производится защита. Кроме традиционных средств мультимедиа для демонстрации презентации, потребуются средства видео и аудио записи для трансляции заседания, а также индивидуальные рабочие станции для каждого члена комиссии с доступом к архивным материалам системы управления обучением. Подобная технология поможет, кроме всего прочего, быстро и качественно провести протоколирование защиты и подведения итогов [11].

Таким образом, модернизация существующей системы высшего образования требует расширения набора информационных технологий, используемых в практике работы вузов. Потребуются организационные изменения в структуре учебных заведений, внедрение компьютерных систем управления учебным процессом, создание новых учебных помещений со специальным оборудованием и программным обеспечением.

СПИСОК ЛИТЕРАТУРЫ

1. Семенова Е.Г. Принципы повышения эффективности образовательного процесса в рамках компетентностного подхода. / Е.Г. Семенова, Е.А. Фролова // Известия ГУАП, 2011, №3, С.83–88.
2. Флегонтов А.В. 10=4+2+4 Информационные системы и технологии / А.В. Флегонтов // Межвузовский сборник научно-технических статей, 2014, №3, С.17–20.
3. Бабаев Б.Д. Вновь о диссертационных делах / Б.Д. Бабаев, В.В. Чекмарёв // Вестник Костромского государственного университета им. Н.А. Некрасова, 2013, Т.19, №3, С.213–216.
4. Немцев А.Н. Информационное обеспечение деятельности диссертационных советов в НИУ «БЕЛГУ» / А.Н. Немцев, А.И. Штифанов, В.А. Беленко и др. // Открытое и дистанционное образование, 2013, №4 (52), С.81–87.

5. Дмитриева А.В. Информационные технологии в бизнес-процессах кафедры вуза / А.В. Дмитриева, А.Г. Степанов // Высшее образование сегодня, 2014, №3, С.42–46.
6. Информационные технологии в работе кафедры / А.Н. Бабенков, В.С. Блюм, С.Д. Бодрунов и др. // под общ. ред. А.Г. Степанова. СПб.: ГУАП, 2014, 276 с.
7. Фомина А.С. Подготовка и проведение учебных мероприятий в режиме видеоконференции в высшем учебном заведении / А.С. Фомина // Электронный журнал «Вестник МГОУ», 2013, Педагогика, №4. [В Интернете]. Available: http://www.evestnik-mgou.ru/Articles/View/500. [Дата обращения: 15.12.2014].
8. Космачев В.М. Организация дистанционного чтения лекций на основе Microsoft Office Live Meeting / В.М. Космачев, А.В. Михеев // Актуальные проблемы экономики и управления, 2014, №1 (1), С.71–75.
9. Крук Б.И. Видео в дистанционном обучении / Б.И. Крук и О.Б. Журавлева // Международный журнал экспериментального образования. Педагогика, 2013, №8, С.28–33.
10. Елина Е.Г. Итоговая государственная аттестация в условиях реализации федерального государственного образовательного стандарта / Е.Г. Елина и А.А. Чувакин // Известия Саратовского университета. Сер. Философия. Психология. Педагогика, 2012, т. 12, №1, С.108–112.
11. Соловьева Н. Рейтинговая оценка выпускной квалификационной работы / Н. Соловьева и М. Крылова // Высшее образование в России, 2007, №9, С.91–94.

УДК 378.14

ВИРТУАЛЬНАЯ СОСТАВЛЯЮЩАЯ НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВУЗА

Тумалева Елена Андреевна,
Российский государственный педагогический университет им. А.И. Герцена,
Россия, Санкт-Петербург, наб. реки Мойки, д. 48,
e-mail: elena_karhu@mail.ru

Аннотация: рассматриваются исследовательские подходы к пониманию сущности феномена «научно-образовательная среда вуза», определяется роль и суть виртуальной составляющей в контексте развития научно-образовательной среды в условиях функционирования трехуровневой системы профессиональной подготовки бакалавриат – магистратура – аспирантура.

Ключевые слова: *научно-образовательная среда вуза; сетевая коммуникация; виртуальная составляющая научно-образовательной среды вуза*

VIRTUAL CONSTITUENT OF SCIENTIFICALLY-EDUCATIONAL ENVIRONMENT OF HIGHER SCHOOL INSTITUTIONS

Elena Tumaleva,
Herzen State Pedagogical University,
Russia, St. Petersburg, Moika, 48,
e-mail: elena_karhu@mail.ru

Abstract: The article highlights the research approaches to the essence of the phenomenon 'scientifically-educational environment of higher school institutions'. It determines the role and functions of the virtual constituent of scientifically-educational environment within the three-level system of professional training – bachelorship – mastership – postgraduate training.

Keywords: *scientifically-educational environment of higher school institutions; network communication; virtual constituent of scientifically-educational environment of higher school institutions*

Введение. Для понимания сущности феномена «научно-образовательная среда вуза» и виртуальная составляющая среды, необходимо обратиться к исследованиям последних лет таких понятий как информационно-образовательная среда, виртуально-образовательная среда. В условиях перехода общества к информационному этапу развития создание информационно-образовательной среды, отвечающей вызовам времени, является одной из ключевых задач Программ развития вузов, поставивших цель создать в рамках вуза среду мирового уровня, которая позволит успешно интегрироваться в мировое образовательное, научное и профессиональное пространство.

Информационно-образовательная среда вуза определяется как программно-телекоммуникационная среда, обеспечивающая едиными технологическими средствами информационную поддержку и организацию учебного процесса, научные исследования, профессиональное консультирование слушателей вуза [1]. Е.В. Трубицина [11] выделяет два основных подхода к определению информационно-образовательной среды. В основу первого, программно-технического, положены информационные, программные и технические ресурсы, объединенные в систему, обеспечивающую эффективное протекание образовательного процесса. Другой подход – социально-педагогический – базируется на таком понятийном аппарате, как «среда», «реальность», «педагогическая система». Структура информационно-образовательной среды представляется при данном подходе значительно более сложной, появляются такие компоненты, как субъектный, содержательный, а программное и аппаратное обеспечение становятся лишь частью саморазвивающейся образовательной среды [11]. Следовательно, при проектировании,

моделировании и развитии среды должны ставиться и решаться не только задачи информационно-программно-технического характера, но и социально-психолого-педагогические и, соответственно, информационно-образовательная среда предстает перед нами как сложное, многокомпонентное системное образование, насыщенное разнообразными ресурсами.

В научной среде широко обсуждается и такой феномен как «виртуальная образовательная среда». Под виртуальной образовательной средой понимается «сетевое коммуникационное пространство, в котором обеспечиваются организация образовательного процесса, его методическая и информационная поддержка, документирование, взаимодействие между всеми субъектами образовательного процесса (студенты, преподаватели, деканат), а также управление им.Виртуальная образовательная среда является частью информационной среды вуза. Для виртуальной образовательной среды, так же как для реальной, важнейшими характеристиками выступают насыщенность (или ресурсный потенциал), а также её структурированность (или способы организации). Кроме того, новым требованием, характерным именно для виртуальной информационной образовательной среды, является учёт следующих важных показателей: степень или уровень локального (субъект-субъектного) взаимодействия всех пользователей среды, а также возможность субъектов преобразовывать (изменять, обогащать) среду, воздействовать на неё» [5].Виртуальная образовательная среда рассматривается либо как совокупность (скорее, система) информационной, технической и учебно-методической подсистем, целенаправленно обеспечивающих учебный процесс, а также его участников, либо как программно-телекоммуникационная среда, обеспечивающая ведение учебного процесса, его информационную поддержку и документирование в электронных сетях с использованием единых технологических средств любому числу учебных заведений, независимо от их профессиональной специализации и уровня образования [6].

Анализ исследований информационно-образовательной среды показывает, что выделенные в них характеристики, могут быть рассмотрены одновременно и как сущностные характеристики научно-образовательной среды современного вуза. Таким образом, научно-образовательная среда современного вуза, интегрируя науку и образование, является неотъемлемой частью социокультурной среды, социокультурного пространства, то есть культуросообразна; строится на гуманистических основаниях, предполагает гуманистический характер взаимодействия субъектов научно-образовательной деятельности; является рефлексивной и инновационной; интегрирует научный, образовательный, инновационный потенциал всех субъектов научно-образовательной деятельности; включает материальную, информационную и виртуальную составляющие как необходимое условие эффективности; является открытой социуму и научно-образовательному сообществу; целенаправленно проектируется и создаётся при активном участии всех субъектов, заинтересованных в её функционировании и развитии [12].

Проанализируем существующие подходы к определению феномена «научно-образовательная среда». Исследователи Юго-Западного государственного университета предложили операционализацию понятия «научно-образовательная среда», которая заключается в следующем понимании её в различных аспектах: «…– сущностном – как синтезированного интегрированного институционального явления, включающего институты науки и образования в их комплексном взаимодействии по осуществлению общепрофильных и обновлённых целей и задач; – процессуальном – как процесс динамической интеграции институтов науки и образования к слиянию в новый единый социальный институт расширенного статусно-функционального содержания.

Научно-образовательная среда, в отличие от научно-образовательной системы, являющейся социальной системой, не так формализована, что выражается в воздействии на неё внешних неучтённых факторов, задающих траекторию её развития, которая может отклоняться от заранее спланированной» [7]. Уточняя определение, данное в работе Жук О. [5], можно рассматривать научно-образовательную среду как «сложную интегративную систему, включающую совокупность всех социальных, материальных, организационно-педагогических и психологических условий и постоянно развивающихся взаимодействий всех участников образовательного процесса (научно-образовательной деятельности – уточн.), направленных на эффективное личностно-профессиональное развитие (профессионалов и – уточн.) будущих специалистов и их самореализацию» [5]. Можно с определёнными уточнениями согласиться с исследователями Красноярского государственного педагогического университета им. В.П. Астафьева [4], которые определяют научно-образовательную среду как особую форму научного сообщества профессионалов и будущих специалистов (студентов и молодых ученых), функционально представляющего собой аналог научной школы. Научно-образовательная среда вуза создаёт условия для развития научного потенциала, академической мобильности и творческой активности студентов (всех субъектов – уточн.). При этом с одной стороны, в процессе взаимодействия субъектов данной среды разрабатываются новые смыслы образования (и научной деятельности – уточн.), апробируются образовательные (и научные – уточн.) технологии; с другой стороны – среда способствует

личностному и профессиональному росту (и профессионально-личностной самореализации – уточн.) её субъектов.

В качестве ещё одного рабочего определения научно-образовательной среды, с определёнными уточнениями, можно также рассматривать следующее: «…распределённое в пространстве сообщество субъектов, заинтересованных в интегративном участии в информационной и научно-педагогической деятельности (в образовательной и научно-исследовательской деятельности – уточн.), обладающих техническими возможностями для такого участия и принимающих в ней активное участие. Решающая роль в развитии и структурировании научно-образовательной среды вуза принадлежит научно-педагогическим школам, выполняющим функции центров кристаллизации научной (научно-образовательной – уточн.) информации в виде парадигмально осмысленного знания и методов его добывания» [8].

В работах ученых Томского политехнического института используется термин интегрированная научно-образовательная информационная среда. Это единая платформа принципов, стандартов, общесистемных требований, а также информационно-программных, компьютерных и телекоммуникационных средств, организационного и методического обеспечения, предназначенная для проектирования прикладных решений по всем направлениям инновационной образовательной программы подготовки элитных специалистов и команд профессионалов мирового уровня [2].

Принципиально важным является вопрос о субъектах научно-образовательной среды. Как видно из приведённых выше определений в них не всегда представлена вся совокупность активных и заинтересованных лиц и объединений субъектов в существовании научно-образовательной среды, которая способна удовлетворить их потребности. По мнению Артюхиной А.И. [3], системно-синергетическое управление научно-образовательным процессом университета обеспечивается: паритетом субъектов в их взаимодействии; совершенствованием управленческого взаимодействия субъектов, направленным на взаимосодействие друг другу в реализации своих полномочий в рамках управления научно-образовательным процессом университета; научно-педагогическим содействием развитию способностей студента (всех субъектов – уточн.) к самостоятельному управлению научно-образовательной деятельностью. В этой связи можно говорить об унитарных субъектах научно-образовательной среды: обучающиеся (студенты, магистранты, аспиранты, докторанты, слушатели); преподаватели; учёные, исследователи, научные сотрудники; административные работники университета; персонал, обеспечивающий научно-образовательную деятельность (лаборанты, инженеры, библиотекари и пр.). Кроме унитарных субъектов следует рассматривать коллективных (совокупных) субъектов: научно-образовательные сообщества и ассоциации, филиалы, институты, научно-образовательные центры, факультеты, кафедры, учебные и научные лаборатории, управления, отделы, службы университета, курсы (потоки) обучающихся, группы обучающихся, объединения обучающихся и преподавателей (исследователей).

Рассматривая структуру многоуровневой научно-образовательной среды инновационного развития вуза, исследователи [8] выделяют в ней следующие компоненты:

- Информационная составляющая среды, которая содержит базу данных конкурсов, проектов и грантов, выполняемых учёными вуза, сведения об объявленных конкурсах, заявках, выполняемых проектах и их результатах, полезных для ведения научных исследовании ресурсах, а также базу данных направлении исследовании, научных школ, исследовательских и творческих групп, ведущих ученых вуза, доступную удалённом пользователям.
- Профессиональные базы знаний и информационные системы, основанные на знаниях, по направлениям подготовки специалистов, отражающим передовые достижения ученых вуза, включая специальные базы знаний для трансфера и коммерциализации инновационных знаний.
- Технологическая и методическая поддержка деятельности по наполнению среды, которая реализуется с помощью информационно-консультационной подсистемы, пополняемой необходимыми ресурсами, содержащими описания структурно-функциональных моделей специализированных баз знаний, технические задания на их развёртывание, методические и учебные материалы по созданию и использованию профессиональных баз знаний.
- Среда сетевых сообществ специалистов.

С помощью данного компонентного состава можно достаточно обобщённо описать научно-образовательную среду. Однако представляется, что его следует дополнить следующими компонентами: человеческие ресурсы (профессорско-преподавательский состав, работники вуза, администрация, обучающиеся); информационные ресурсы (информационно-исследовательский, информационно-библиотечный ресурс, информационно-образовательный ресурс и др.); ценностные характеристики корпоративной культуры субъектов научно-образовательной среды; коммуникативные отношения субъектов научно-образовательной (различные виды взаимодействия) [12].

Любая организация, в том числе и вуз, находится и функционирует в рамках внешней и внутренней сред, которые предопределяют успешность функционирования. Внешняя среда вуза является источником, питающим организацию ресурсами, необходимыми для поддержания её

внутреннего потенциала на должном уровне, а внутренняя определяет технические и организационные условия работы и является результатом управленческих решений.

На характер внешних связей научно-образовательной среды вуза оказывает влияние ряд факторов: сложившийся рынок труда в России и в регионе; профиль вуза, определяющий систему взаимоотношений с базовыми предприятиями, организациями, учреждениями и использование их баз и кадрового потенциала для подготовки специалистов; специфика специальности, определяющая взаимодействие с рядом организаций определённой направленности, которые одновременно предоставляют возможности для прохождения практики на их базе, что позволяет расширить возможности выпускников в реализации себя в дальнейшей профессиональной деятельности; молодёжная политика органов государственной власти на региональном и городском уровне. Внешняя среда любой организации, в том числе и вуза, является весьма неоднородной. С точки зрения интенсивности взаимодействия организации с внешним окружением принято выделять три среды воздействия: локальная (среда прямого воздействия); глобальная (среда косвенного воздействия); международная [9].

Склярова Т.В. [10], изучая социокультурную среду учреждений высшего профессионального образования, ввела понятие образовательного инвайронмента (от англ. environment – среда, окружение), которое описывает внутреннюю и внешнюю среду образовательного учреждения, рассматриваемую на микро-, мезо-, макро и экзо уровнях. В связи с взаимодействием научно-образовательной среды с внешней и внутренней средой (структурой) на выделенных уровнях уместно говорить о *функциях*, которые реализует в своей деятельности научно-образовательная среда. Следуя данному подходу, можно предположить какие функции может реализовывать научно-образовательная среда. На микроуровне (унитарные субъекты, деятельности и межличностные взаимодействия субъектов) научно-образовательная среда может реализовать следующие функции: интегративная, ценностно-согласовательная, фундаментализирующая, коммуникационная, информационная, образовательная, воспитательная, развивающая, адаптационная, социализирующая и др. На мезоуровне (совокупные субъекты: институты, факультеты, кафедры, деканаты, управления, отделы, службы и пр.) реализуются следующие функции: интегративная, координационная, организационная, проектировочная, управленческая, информационная, диагностическая, аналитическая и др. На макроуровне (внешние для вуза социально-экономические, социокультурные условия, потребители, работодатели, глобальные процессы и пр.) научно-образовательная среда может реализовать следующие функции: инновационная, научно-исследовательская, маркетинговая, экспертная, внедренческая, интернационализации результатов научно-образовательной деятельности и др. На экзоуровне (институты и процессы, в которые субъекты научно-образовательной среды не включаются непосредственно, но которые могут опосредованно оказывать воздействие на них: социокультурная среда, средства массовой информации, рейтинги и пр.): культуротворческая, социокультурная, научно-исследовательская, прогностическая, просветительская, пропагандистская, презентационная и др.

Процесс формирования научно-образовательной среды целесообразно рассматривать с системных позиций, при этом можно выделить: модель формирования, проектирование; условия формирования; основные факторы и аспекты формирования; последовательность этапов или конкретных мероприятий. Таким образом, научно-образовательная среда предстает перед нами как сложное, многокомпонентное системное образование, насыщенное разнообразными ресурсами (научными, учебными, учебно-методическими). В совокупности ресурсы направлены на достижение целей образования. Можно определить научно-образовательную среду как часть глобальной научно-образовательной среды, часть социокультурного пространств и зону взаимодействия элементов образовательной системы и науки, образовательного материала и субъектов образовательного процесса, оптимально структурированную среду, реализующую технологическими средствами и взаимосвязанным адекватным содержательным наполнением качественное обучение и предоставляющую возможность для исследовательской деятельности. Подобная среда должна включать в себя организационно-методические средства, совокупность технических и программных средств хранения, обработки, передачи информации, обеспечивающую оперативный доступ к значимой информации и создающую возможность для общения не только субъектов научно-образовательной среды вуза, но и возможных субъектов глобальной коммуникации.

Формирование и развитие научно-образовательной среды современного вуза сегодня происходит в условиях функционирования трехуровневой системы профессиональной подготовки бакалавриат – магистратура – аспирантура, поэтому вектор трансформации научно-образовательной среды в настоящее время сопровождается многообразными организационными переменами и пересмотром её сущностных характеристик, структуры и содержательного наполнения. В контексте реформирования научно-образовательной среды приоритетными становятся задачи гибкого управления интеллектуальными и материальными ресурсами, стимулирования инноваций, позиционирования на рынке образовательных услуг и т.д., а, следовательно, развитие виртуальной составляющей научно-образовательной среды.

Под виртуальной составляющей научно-образовательной среды вуза будем понимать сетевое коммуникационное пространство, в котором обеспечиваются организация научного и образовательного процессов, информационная и методическая поддержка, удовлетворение информационно-коммуникативных потребностей научных сотрудников, преподавателей, студентов, администрирование, взаимодействие между всеми субъектами научно-образовательного процесса, а также управление ими. Виртуальная составляющая научно-образовательной среды создается и развивается для эффективной коммуникации всех ее участников. Следует отметить, что каждый инновационный ресурс, используемый в виртуальной среде, имеет свои сильные и слабые технологические стороны. Гибкая комбинация применяемых инструментов/ресурсов/инновационных продуктов позволяют повысить эффективность виртуальной составляющей научно-образовательной среды. Научно-образовательную среду следует определять как часть глобальной среды, часть социокультурного пространства и зону взаимодействия научно-образовательных ресурсов и субъектов среды, оптимально структурированную и методически организованную среду, реализующую технологическими средствами и взаимосвязанным адекватным содержательным наполнением качественное обучение и исследовательскую деятельность. Подобная среда должна включать в себя организационно-методические средства, совокупность технических и программных средств хранения, обработки, передачи информации, обеспечивающую оперативный доступ к значимой информации и создающую возможность для общения не только субъектов внутри вуза, но и возможных субъектов глобальной коммуникации в образовательной и научных сферах.

Мультимедийная гипертекстовая среда идеальна для реализации целого ряда задач, стоящих перед любым учебным заведением: использование дистанционных технологий и электронного обучения обучение в самом широком понимании этих процессов; хранение и представление мультимедийных научных и учебных материалов; администрирование базы учебных и научных материалов, их разработка и корректировка; доступ к информационному фонду, как данного вуза, так и всей информации, доступной в глобальной сети; обеспечение оперативного взаимодействия обучаемого и преподавателя, научного сотрудника. Кроме того, такая среда позволяет: организовывать индивидуальное обучение и самостоятельную научно-исследовательскую работу и управлять этими процессами; создавать учебно-методические комплексы нового поколения; использовать видеоконференцсвязь для организации внутриинститутских телеконференцийи межвузовского общения; совершенствовать систему электронного документооборота и т.д. В результате анализа можно определить основные компоненты образовательной среды: система администрирования; электронная библиотека научных, учебных и учебно-методических ресурсов; банк компьютерных обучающих и исследовательских программ; телекоммуникационная инфраструктура.

Одним из подходов к развитию виртуальной составляющей научно-образовательной среды вуза может выступать децентрализация управления ею и изменение позиции студентов, преподавателей и научных сотрудников из пассивных объектов ее воздействия в активно изменяющих и создающих ее элементы субъектов, что будет способствовать более успешному протеканию самоорганизационных процессов и развитию самой среды. Важным условием эффективного функционирования виртуальной составляющей является превращение ее в открытую самоорганизующуюся систему, в том числе за счет взаимодействия с работодателями; предоставления студентам возможности управлять процессом обучения (прежде всего организации научно-исследовательской работы и практик), принимая участие в его планировании и оценке качества, осуществлять самоконтроль и самооценку. Функционирование такой открытой самоорганизующейся виртуальной составляющей научно-образовательной среды вуза может стать основой академической и научной мобильности всех участников научного и образовательного процессов в вузе, а также средством усиления субъектной позиции студентов в обучении.

Заключение. Данная проблема в настоящее время является направлением исследования по проекту 2.1.1. «Комплексное исследование особенностей научно-образовательной среды современного университета в контексте отечественного и зарубежного опыта на базе НИИ НПО» Программы стратегического развития РГПУ им. А.И. Герцена на 2012–2016 годы.

СПИСОК ЛИТЕРАТУРЫ

1. Абросимов А.Г. Информационно-образовательная среда вуза. «Вестник РУДН» серия «Информатизация образования», 2004, №1. [Электронный ресурс] Режим доступа: http://cis.rudn.ru/document/show.action;jsessionid=323ABCF22F39FB380B9404A89A8F1D69?document.id=558
2. Агранович Б.Л., Похолков Ю.П., Ямпольский В.З. Интегрированная научно-образовательная информационная среда национального исследовательского Томского политехнического университета//Материалы научно-методической конференции «Современные информационные технологии в образовании: Южный федеральный округ» 11–13 мая 2011. Ростов-на-Дону, 2011. [Электронный ресурс] Режим доступа: http://conf.sfedu.ru/inftech2011/pres/sbornikSITO2011.pdf
3. Артюхина А.И. Образовательная среда высшего учебного заведения как педагогический феномен (на материале проектирования образовательной среды медицинского университета): Дисс. доктора педагогических наук: 13.00.08 / Артюхина Александра Ивановна; [Место защиты: ГОУВПО «Волгоградский государственный педагогический университет»] – Волгоград, 2007, 377с. [Электронный ресурс] Режим доступа: http://www.bestreferat.ru/referat-136354.html

4. Бандурина И.А. Научная школа как среда развития этических ценностей научной молодежи в эпоху глобализации: Автореф. дисс канд. педагогических наук. – Ростов-на-Дону, 2010.
5. Жук О.Л. Виртуальная образовательная среда вуза как фактор личностно-профессионального развития будущего специалиста / О.Л. Жук, С.Н. Сиренко // Педагогическата среда в университета като пространство за професионално-личностно развитие на бъдещия специалист: в 2 Т.: сб. науч. ст: – Габрово, ЕКС-ПРЕС, 2011, Т.1, С133–137.
6. Ильченко О.А. Организационно-педагогические условия сетевого обучения. – М., 2002, 272с.
7. Кравчук П.Ф., Боев Е.И., Шуклина О.С. Научно-образовательная среда в контексте инновационного развития: теоретико-методологические основания исследования // Известия Юго-Западного государственного университета. 2011, №2, С.91а-97. [Электронный ресурс] Режим доступа: http:// http://elibrary.ru/item.asp?id=16516684
8. Левченко Д.В., Унайсарова Р.Д. Формирование научно-информационного пространства высшего учебного заведения. [Электронный ресурс] Режим доступа: ttp://sioi.conf.udsu.ru/report?node=1252609136
9. Леонтьева О.А. Внутренняя среда вуза: механизмы трансформации изменений внешней среды в идеологические инновации //Экономические науки, №12, 2007.
10. Склярова Т.В. Социокультурная среда высшего образования: Автореф. дисс. канд. соц. наук. – Саратов, 1998, 17с.
11. Трубицина Е.В. Два подхода к определению информационно-образовательной среды // Материалы VI Всероссийской научно-практической конференции «Применение информационно-коммуникационных технологий в образовании». – Марий Эл, 2009, С.34–37
12. Тумалева Е.А., Эхов С.Ф. Теоретические основы формирования и развития научно-образовательной среды современного университета. [Электронный ресурс] The Emissia.Offline Letters Электронное научное издание (научно-педагогический интернет-журнал) Режим доступа: http://www.emissia.org/offline/2013/2003.htm

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ

УДК: 378.1, 001.89

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

Абрамян Геннадий Владимирович,
Российский государственный педагогический университет им. А.И. Герцена,
Россия, Санкт-Петербург, наб. р. Мойки, 48,
e-mail: ict@fit-herzen.ru

Аннотация: в статье рассматриваются риски и информационные угрозы научно-образовательной среды Российской Федерации в условиях использования компьютерных систем и технологий электронного обучения на платформе WINDOWS.

Ключевые слова: *информационные угрозы; объекты риска; технологии электронного обучения; научно-образовательная среда.*

RISKS AND POTENTIAL THREATS TO COMPUTER SYSTEMS AND E-LEARNING TECHNOLOGIES ON WINDOWS PLATFORM SCIENTIFIC AND EDUCATIONAL ENVIRONMENT OF THE RUSSIAN FEDERATION

Gennady Abrahamian,
Russia, St. Petersburg, Herzen State Pedagogical University of Russia,
e-mail: ict@fit-herzen.ru

Abstract: The article describes the risks and threats of scientific information and educational environment of the Russian Federation in the conditions of use of computer systems and technologies of e-learning platform WINDOWS.

Keywords: *threat information ; risk facilities ; e-learning technologies ; Research and Educational Environment.*

Введение. 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. [1], [2]. 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 [4], [6] 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 [7], [8].

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 риска научно-образовательной и информационной безопасности вузов и школ РФ [3].

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] 3) сотрудничество с европейским сообществом в области науки, воспитания и образования в соответствии с европейскими ценностями и стандартами «открытого образования». [4], [5]. 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:

– среды одновременного, отложенного, локального и глобального доступа, передачи, хранения или обработки научной, учебной, технической информации-контента;

– в среде управления содержанием деятельности или документооборота, например в среде научных исследований, электронного обучения, а также несанкционированного доступа к персональным данным (информации) субъекта КСИТЭО;

– 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 КСИТЭО на платформе WINDOWS;

– уровней публичного и закрытого взаимодействия, секретности, целостности, доступности, штатной работы НОУ или субъектов КСИТЭО на платформе WINDOWS;

– уровней физической и технической инфраструктуры НОУ или КСИТЭО на платформе WINDOWS;

– уровней программного обеспечения КСИТЭО НОУ или субъекта КСИТЭО на платформе WINDOWS;

– уровней кадровых ресурсов функционирования КСИТЭО на платформе WINDOWS НОУ или дефицита компетенций сотрудников, преподавателей или обучаемых;

– нормативно-юридических уровней обеспечения работы КСИТЭО на платформе WINDOWS;

– организации научно-методической деятельности КСИТЭО на платформе WINDOWS;

– организационно-административной деятельности КСИТЭО на платформе WINDOWS;

– организации научной и психолого-педагогической поддержки субъектов КСИТЭО на платформе WINDOWS,

– медико-биологического и экологического состояния инфраструктуры организаций использующих КСИТЭО на платформе WINDOWS;

– финансово-экономических ресурсов организаций, научных и образовательных сообществ, а также возможностей сотрудника или обучаемого на основе КСИТЭО на платформе WINDOWS;

– в среде и инфраструктуре социальных, политических и государственных образований российского общества, в том числе непосредственно внедряющих и поддерживающих технологии КСИТЭО на платформе WINDOWS.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамян Г.В. Модели научного сотрудничества и профессионального образования в информационной среде стран Азиатско-Тихоокеанского экономического сотрудничества (АТЭС). В сборнике: Информационно-телекоммуникационные системы и технологии» (ИТСиТ-2014) Материалы Всероссийской научно-практической конференции. Кемерово, 2014. С. 7–8.
2. Абрамян Г.В. Система международного научного сотрудничества и модели глобализации профессионального образования и науки в информационной среде стран БРИКС. В сборнике: Региональная информатика «РИ-2014» материалы XIV Санкт-Петербургской международной конференции. 2014. С. 290-291.
3. Абрамян Г.В. Системы и технологии электронного обучения как потенциальные объекты риска информационно-образовательной среды вузов и школ Российской Федерации. В сборнике: Электронное обучение в вузе и школе материалы сетевой Международной научно-практической конференции. Российский государственный педагогический университет им. А.И. Герцена. 2014. С. 17-20.
4. Абрамян Г.В., Катасонова Г.Р. Переходные и стационарные алгоритмы обеспечения континуальной квазиустойчивости системы непрерывного образования в условиях бинарно-открытого информационного пространства и связей на основе механизмов откатов. Фундаментальные исследования. 2015. № 2-26. С. 5884-5890.
5. Деревянко Ю.Д., Принцев А.С., Соколов Н.Е. Принципы создания и развития системы менеджмента качества современного вуза. Финансы, деньги, инвестиции. 2013. № 1 (45). С. 035-038.
6. Изранцев В.В., Принцев А.С., Соколов Н.Е. Опыт создания и развития единой электронной образовательной среды МБИ Банковские услуги. 2013. № 4. С. 023-028.
7. Соколов Н.Е. Методика компьютерного адаптивного тестового контроля знаний учащихся (в курсе информатики) диссертация на соискание ученой степени кандидата педагогических наук / Санкт-Петербург, 2000
8. Раскин В.Н. Психологические факторы успешности учебной и научной работы аспирантов технического вуза. Автореферат диссертации на соискание ученой степени кандидата психологических наук. – СПб: ЛГУ, 1992. 16 с.

УДК 006.015.2

ПЕРСПЕКТИВЫ РАЗРАБОТКИ И АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

Буйневич Михаил Викторович,
Бучкова Евгения Сергеевна, Быстрова Ольга Денисовна,
ЗАО «Ассоциация специалистов информационных систем»,
Россия, Санкт-Петербург, ул. Кантемировская, д.7,
e-mails: Geshinka@gmail.com, bystrova.o.d@mail.ru

Аннотация: В статье рассмотрены вопросы актуальности разработки и внедрения профессиональных стандартов, их применение и соотношения с действующими образовательными стандартами.

Ключевые слова: *профессиональный стандарт; практические навыки; знания; трудовая деятельность; образование.*

PERSPECTIVE OF DEVELOPMENT AND RELEVANCE OF IMPLEMENTATION OF PROFESSIONAL STANDARDS

Buinevich Mikhail V., Olga Bystrova, Eugeniya Buchkova,
Information Systems Specialists Association,
Russia, St. Petersburg, Kantemirovskaya str. 7,
e-mails: bystrova.o.d@mail.ru, Geshinka@gmail.com

Abstract: The article presents problems of topicality development and implementation of professional standards, their application and correlation with actual educational standards.

Keywords*: professional standards; practical skills; knowledge; working career; education.*

Введение. 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. В этих условиях возникает проблема разрозненности требований различных организаций к знаниям, умениям и компетенциям потенциальных работников, желающих занять ту или иную должность. В связи с этим проявляется 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.

Помимо вышеперечисленных факторов ситуацию обостряет нестабильная политическая обстановка в мире. Она усиливает миграционные потоки в обществе, что приводит к увеличению в нашей стране доли населения с различным, часто низким, уровнем образования.

Профессиональные стандарты, имеющие широкое практическое применение за рубежом, устанавливают требования к знаниям, умениям и практическим навыкам, определяющим обязательные компетенции, которые требуются для исполнения определенных работ или обязанностей. В данный момент они рассматриваются как мощный инструмент, позволяющий создать прочное взаимодействие сфер труда и образования, обеспечивающий все условия для рационального использования людских ресурсов.

Для описания сути и применения профессиональных стандартов были использованы понятия «квалификация работника» и «профессиональный стандарт», определения которых приведены в статье 195.1 Трудового Кодекса Российской Федерации «Понятия квалификации работника, профессионального стандарта». В соответствии с вышеуказанной статьей, квалификацию работника определяют как уровень знаний, умений, профессиональных навыков и опыта практической работы работника. В свой черед, профессиональным стандартом называют характеристику квалификации, которая обязательна для работника, осуществляющего конкретный вид профессиональной деятельности.

В январе 2013 года Правительство РФ утвердило правила разработки, закрепления и использования профессиональных стандартов. Приказом Министерства Труда и Социального Развития были определены структура и внешний вид профессионального стандарта. В свою очередь, их конструкция и внутреннее содержание очень широко варьируется и зависит от большого количества различных факторов. К ним можно отнести направление и характер профессиональной деятельности, четко определенные задачи, которые данный стандарт призван решить и, конечно же, методы создания стандартов.

В теории, можно выявить несколько возможных положительных последствий введения профессиональных стандартов. Во-первых, данные нормативные документы способны оказать помощь выпускникам школ в процессе профориентации – при выборе будущей профессии. Так как профессиональные стандарты, в идеале, должны четко отражать, какими знаниями, навыками и умениями должен обладать будущий сотрудник, школьникам будет гораздо легче определиться с направлением своей будущей учебы и выбором ступени дальнейшего образования: поступать ли ему в колледж и получать среднее специальное образование, достаточным ли будет квалификация бакалавра или же придется поступать и в магистратуру. Так же проще будет проводить профориентационную работу в соответствующих учреждениях и на курсах профориентации. В своей работе специалисты смогут ссылаться на реально существующие официальные стандарты.

В свою очередь, студентам высших учебных заведений будет легче определяться с направлением дальнейшей профессиональной деятельности. Так как в профессиональных стандартах будут четко прописаны требования к будущим сотрудникам, студенты станут более четко представлять, на каких сферах знаний стоит сфокусировать особое внимание во время учебного процесса.

Во-вторых, профессиональные стандарты должны унифицировать требования к специалистам различных должностей. Как было отмечено выше, в данных нормативных документах должны отмечаться не только требования к уровню образования будущего сотрудника организации, но и четкий список практических навыков и знаний, которыми он должен обладать. Отсюда возникает вопрос, ответ на который пока не найден – как в современном обществе, с его стремительно развивающимися технологиями, создать профессиональный стандарт, который не требовал бы постоянной доработки?

В-третьих, очень своевременным является ввод профессиональных стандартов в переходный период для высшего образования, когда отмирает старая форма подготовки специалистов и вводится новая модель, разделенная на две части: подготовку бакалавров и магистров. Данные нормативные документы сориентируют не только студентов, но и самих работодателей, так как в них будет прописано, с какими задачами способен справляться выпускник, освоивший ту или иную ступень образования, и насколько ответственную работу ему можно поручить.

Стоит упомянуть о болезненности ввода бакалавриата и магистратуры в России. До сих пор происходит переход от старой формы получения высшего образования, к новой, разделенной на две ступени. К сожалению, до сих пор никем официально не определено, сколько лет необходимо на обучение специалистов той или иной профессии, и достаточно ли для получения высшего образования четырех лет обучения. На наш взгляд, время обучения и сама учебная программа должны определяться компетенциями, выстроенными на базе профессиональных стандартов.

На текущий момент компетенции, на основе которых выстраивается обучение молодого специалиста, до сих пор не имеют под собой какой-либо официальной основы. На момент создания компетенций, отражающих навыки и умения, которыми должен обладать выпускник высшего учебного заведения, еще не были разработаны профессиональные стандарты. Следовательно, возникают вопросы: на основе чего были созданы компетенции? Будут ли они модифицированы после введения

профессиональных стандартов? Если это произойдет и компетенции будут отредактированы в соответствии с профессиональными стандартами, тогда, на наш взгляд, требования к уровню образования молодых специалистов значительно возрастет. Если же трудовые стандарты будут разработаны в соответствии с уже имеющимися компетенциями, то, вполне возможно, уровень образования выпускников не будет соответствовать ожиданиям работодателей.

Не удивительно, что данная тема вызывает все больший интерес со стороны будущих работодателей. В то же время сфера образования начинает прислушиваться к потребностям рынка труда и тем требованиям, которые предъявляются к выпускникам ВУЗов. Не смотря на то, что их функции, по факту, заканчиваются на этапе выпуска дипломированных специалистов.

Необходимо, чтобы нынешние государственные федеральные стандарты образования соответствовали актуальным требованиям работодателей, представленных в форме профессиональных стандартов. Опираясь на зарубежный опыт, можно отметить, что обобщение требований работодателей трудоемкий и крайне сложный процесс, который зависит от многих факторов, включая характер взаимодействия системы профессионального образования и рынка труда. Для этого применяется метод функционального анализа, являющий собой проведение опросов большого числа предприятий определенной отрасли, учет тенденций ее развития. 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.

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. Загадкой также остается и сам процесс проверки знаний выпускников. Как именно это должно выглядеть? В какой форме должна проводиться проверка? Где найти достаточное количество компетентных специалистов и как они будут справляться с огромным потоком выпускников? Где будет проходить отбор – на биржах труда или на самих предприятиях? Может быть 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. Но как тогда отследить адекватность и корректность проверки знаний? Все эти вопросы пока остаются без ответов.

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 – как системы образования, так и работодателей, и обучающихся.

УДК 338.28

ТРЕБОВАНИЯ К АККРЕДИТАЦИИ КОМПАНИЙ, ЗАНИМАЮЩИХСЯ АУДИТОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Солодянников Александр Владимирович, Пилипов Михаил Васильевич,
Федоров Дмитрий Юрьевич,
ЗАО «Ассоциация специалистов информационных систем»,
Россия, Санкт-Петербург, ул. Кантемировская, д. 7,
e-mails: a.solodyannikov@spbissa.ru, m.pilipov@spbissa.ru, dmitriy.fedoroff@gmail.com

Аннотация: В данной статье рассмотрены основные требования к аккредитации организаций, предоставляющих услуги аудита информационной безопасности, существующие в настоящее время.

Ключевые слова*: информационная безопасность, информационные системы, аудит информационной безопасности.*

REQUIREMENTS FOR ACCREDITATION OF COMPANIES INVOLVED IN THE INFORMATION SECURITY AUDIT

Solodyannikov Alexander Vladymyrovich, Pilipov Mikhail Vasilyevich,
Fedorov Dmitriy Yuryevich,
«Association of specialists of information technology»,
Russia, St. Petersburg, st.Kantemyrovskaya, 7,
e-mails: a.solodyannikov@spbissa.ru, m.pilipov@spbissa.ru, dmitriy.fedoroff@gmail.com

Abstract: This article discusses the basic requirements for accreditation of organizations providing services of audit of information security available today.

Keywords: *Information security, information systems, audit of information security.*

В соответствии с требованиями законодательства РФ, любая организация, использующая в своей деятельности какие-либо конфиденциальные данные, обязана обеспечивать безопасность их обработки и хранения.

Аудит информационной безопасности позволяет получить независимую качественную и количественную оценку защищенности корпоративной информационной системы, оценить ее соответствие предъявляемым нормативным и корпоративным требованиям безопасности.

Аудит информационной безопасности включает:

– Анализ защищенности информационных систем;
– Анализ угроз нарушения информационной безопасности;
– Оценку информационных рисков и воздействия на бизнес;
– Оценку соответствия требованиям стандартов;
– Аттестацию и сертификацию по требованиям безопасности информации РД ФСТЭК России.

Зачастую компании не имеют собственных квалифицированных специалистов, способных провести оценку имеющейся информационной системы, и отдают этот вид деятельности на аутсорсинг.

Прежде чем заниматься аудитом информационной безопасности, организация должна пройти аккредитацию на проведение сертификационной оценки.

Еще несколько лет назад не существовало четких требований к компаниям, осуществляющим аудит информационной безопасности.

В данной статье рассмотрены основные требования к аккредитации организаций, предоставляющих услуги аудита информационной безопасности, существующие в настоящее время.

В первую очередь компания должна иметь лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

Под технической защитой конфиденциальной информации понимается выполнение работ или оказание услуг, определенных Постановлением Правительства РФ от 3 февраля 2012 г. № 79, в том числе аттестационные испытания и аттестация на соответствие требованиям по защите информации.

На сайте ФСТЭК можно найти и скачать реестр лицензий на деятельность по технической защите конфиденциальной информации, который содержит номера выданных лицензий, дату выдачи, срок действия, наименование лицензиата, адрес места нахождения и осуществления деятельности.

Лицензия ФСТЭК требует наличия у организации действующей лицензии ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну.

Также организация, занимающаяся аудитом информационной безопасности должна осуществлять свою деятельность в соответствии со стандартом ГОСТ Р ИСО/МЭК 27006-2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

Данный стандарт устанавливает требования к организациям, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности. Он также может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки и других процессов аудита.

Требования ГОСТа Р ИСО/МЭК 27006-2008 содержат нормативные ссылки на следующие стандарты:

– ИСО/МЭК 17021:2006 «Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента»;
– ИСО/МЭК 27001:2005 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
– ИСО/МЭК 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

Одной из важных особенностей стандарта является наличие требований к компетентности персонала компании, занимающейся аудитом информационной безопасности.

– Знание стандарта СМИБ и других соответствующих нормативных документов;
– Понимание вопросов информационной безопасности;
– Понимание оценки риска и менеджмента риска с точки зрения деятельности;
– Технические знания о деятельности, подлежащей аудиту;
– Общие знания нормативных требований, относящихся к СМИБ;
– Знание систем менеджмента;
– Понимание принципов аудита, основанных на ИСО 19011:2002;
– Знание анализа эффективности СМИБ и измерения эффективности средств контроля.

Для компаний, занимающихся аудитом информационной безопасности банков, являются существенными следующие документы:

– Комплекс документов Банка России СТО БР ИББС;

– Стандарт PCI DSS;
– Федеральный Закон от 27 июня 2011 г. № 161 –ФЗ «О национальной платёжной системе».

Стандарт СТО БР ИББС описывает единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства. Вопросы аудита и оценки соответствия требованиям стандарта прописаны в отдельных документах — «СТО БР ИББС-1.1-2007. Аудит информационной безопасности», «СТО БР ИББС-1.2-2010. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2010» и «РС БР ИББС-2.1-2007. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

Стандарт PCI DSS (PaymentCardIndustryDataSecurityStandard) – стандарт безопасности данных платежных карт, разработанный Советом по стандартам безопасности индустрии платежных карт (PaymentCardIndustrySecurityStandardsCouncil, PCI SSC), который был учрежден международными платежными системами Visa, MasterCard, AmericanExpress, JCB и Discover. Стандарт PCI DSS представляет собой совокупность 12 высокоуровневых и свыше 200 детальных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационных системах организаций. Требования стандарта распространяются на все компании, работающие с международными платежными системами Visa и MasterCard.

Выше были рассмотрены основные требования в области информационной безопасности, касающиеся аудиторских организаций. Однако, несмотря на наличие данных требований в стране до сих пор отсутствуют унифицированные подходы к регуляции деятельности фирм, занимающихся аудитом информационной безопасности.

УДК 51-7
ГРНТИ 1401.77

К ВОПРОСУ ПРИМЕНЕНИЯ СТАТИСТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ ЗНАНИЙ КУРСАНТОВ ПО УЧЕБНЫМ ДИСЦИПЛИНАМ НАПРАВЛЕНИЯ ПОДГОТОВКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» В УЧЕБНЫХ ЗАВЕДЕНИЯХ СИСТЕМЫ МВД РОССИИ

Бобонец Сергей Алексеевич[1], Куватов Валерий Ильич[2], Примакин Алексей Иванович[2],
[1]Санкт-Петербургский военный институт внутренних войск МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
[2]Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
e-mails: sbobon@mail.ru, kyb.valery@yandex.ru, a.primakin@mail.ru.

Аннотация: В статье представлены результаты исследований, проводимых сотрудниками кафедры обеспечения служебно-боевой деятельности внутренних войск Санкт-Петербургского военного института ВВ МВД России и кафедры специальных информационных технологий Санкт-Петербургского университета МВД России. Предложена модель оценки результатов тестирования знаний курсантов, в основе которой лежит теория проверки статистических гипотез. Модель позволяет проанализировать результаты тестирования и оценить (при заданном уровне значимости) на сколько вопросов теста тестируемый ответил правильно потому, что он эти ответы знал и сколько правильных ответов он угадал.

Ключевые слова: *тестирование; статистическая модель; биномиальный закон; статистическая гипотеза; уровень значимости.*

THE ISSUE OF APPLICATION OF STATISTICAL MODEL FOR EVALUATING TESTING OF KNOWLEDGE ON A SUBJECT MATTER CADETS TRAINING AREAS «INFORMATION SECURITY» IN THE EDUCATIONAL INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS RUSSIA

Bobonets Sergey Alekseevich[1], Kuvatov Valery Ilich[2], Primakin Alex Ivanovich[2],
[1]Sankt Petersburg Military Institute of Internal Troops of Russia,
Russia, Saint-Petersburg, street Flyer Pilyutova, d. 1,
[2]Sankt Petersburg University of the Russian Interior Ministry,
Russia, Saint-Petersburg, street Flyer Pilyutova, d. 1,
e-mails: sbobon@mail.ru, kyb.valery@yandex.ru, a.primakin@mail.ru.

Abstract: the article presents the results of research conducted by members of the Department provide service and combat activity of the internal troops of the St. Petersburg military Institute of internal troops of Russia and the Department of information technologies, St. Petersburg University of the Ministry of internal

Affairs of Russia. The model of evaluation of the results of testing students ' knowledge, which is based on the theory of statistical hypothesis testing. The model allows to analyze the test results and evaluate (at a given significance level) on how many test questions test answer correctly because the answers he knew and how many correct answers he guessed.

Keywords*: testing; statistical model; binomial law; statistical hypothesis; level of significance.*

Министр внутренних дел РФ поставил перед ВУЗами МВД задачу значительного повышения качества подготовки офицеров. Качество подготовки офицеров во многом определяется качеством контроля степени усвоения учебного материала.

В высшей школе существует достаточно много форм и методов контроля. Однако в большинстве из них оценку дает тот же преподаватель, который обучал данному предмету. Такой подход вызывает определенные сомнения в объективности оценки. Этого недостатка лишен тестовый контроль.

Помимо этого, роль тестового контроля значительно возрастает при модульной организации построения основных образовательных программ, о чем особо указывается в Федеральном законе 273-ФЗ РФ «Об образовании в Российской Федерации», вступившего в силу с 1 сентября 2013 года [1]. Применение блочно-модульных технологий при построении учебных планов, формирование оптимальной последовательности освоения соответствующих модулей [2], [3] предполагают, что по завершению изучения каждого модуля знания учащегося необходимо оценить. Решение данной задачи возлагается на тестовый контроль [4].

Тесты, особенно с применением компьютерных технологий, позволяют в максимальной степени формализовать процесс оценки знаний при значительном сокращении длительности этого процесса. Оценка результатов тестирования обычно проводится по схеме: «неудовлетворительно» ставится, если тестируемый показал менее 30% правильных ответов, «удовлетворительно» – если от 30% до 50% правильных ответов, «хорошо» – если от 50% до 80%, «отлично» – если 80% и более.

Цифры могут быть и другими, но суть данной схемы остается прежней. Эта схема не учитывает общего числа вопросов теста и вероятности того, что правильные ответы на некоторые вопросы теста могут быть получены случайно – в результате угадывания.

Ниже предлагается подход, основанный на теории проверки статистических гипотез [5], свободный от указанных недостатков.

Пусть число вопросов теста равно n, в каждом вопросе предлагается υ вариантов ответа, один и только один из которых является правильным, и тестируемый правильно ответил на m вопросов из n. Необходимо разработать статистическую модель, с помощью которой можно было бы определить, на сколько вопросов тестируемый ответил правильно потому, что знал ответы, а сколько правильных ответов он угадал.

Если тестируемый знает ответ на вопрос, он отвечает на него правильно. Если тестируемый не знает ответ на вопрос, то он отвечает на него правильно с вероятностью угадывания равной:

$$P = \frac{1}{\upsilon}. \tag{1}$$

Очевидно, что закон распределения числа угаданных ответов является биномиальным [6].

Пусть курсант не знает правильного ответа ни на один вопрос теста. Вероятность того, что он угадает ровно b правильных ответов, определяется по формуле:

$$P(n,b) = P_y^b (1 - P_y)^{n-b}. \tag{2}$$

Зададимся доверительной вероятностью α. Найдем максимально возможную величину m, которая еще удовлетворяет условию:

$$\sum_{i=m}^{n} C_n^i P_y^i (1 - P_y)^{n-i} \geq \alpha. \tag{3}$$

Формула (3) позволяет вычислить пороговое значение числа правильных ответов – m из n, при котором мы еще можем допустить, что все ответы тестируемый *угадал*, т.е. такое m, что соотношение (3) справедливо для m и несправедливо для $m+1$. Следовательно, если количество правильных ответов тестируемого b меньше, чем m, то с доверительной вероятностью мы можем сказать, что он все эти ответы угадал, если же b, то ответ хотя бы на один вопрос теста он знал.

Пусть тестируемый в ходе эксперимента правильно ответил на b вопросов. Выдвинем две гипотезы, основную:

– H_0 – тестируемый не знает ответа ни на один из вопросов теста, и все b правильных ответов угадал, и альтернативную:

– H_1 – тестируемый знает ответ хоть на один из тех b вопросов теста, на которые он ответил правильно.

Если b меньше или равно m, то из формулы (3) следует:

$$\sum_{i=b}^{n} C_n^i P_y^i (1-P_y)^{n-i} \geq \alpha, \tag{4}$$

и мы с доверительной вероятностью α можем утверждать, что гипотеза H_0 не противоречит результатам эксперимента, то есть тестируемый не знает правильный ответ ни на один вопрос теста и все правильные ответы им угаданы. На этом анализ результатов тестирования закончен.

Если b больше m, то из формулы (3) следует:

$$\sum_{i=b}^{n} C_n^i P_y^i (1-P_y)^{n-i} < \alpha, \tag{5}$$

и мы с доверительной вероятностью a можем утверждать, что гипотеза H_0 неверна, верна альтернативная гипотеза N_1, и тестируемый знает правильный ответ, хотя бы на один из тех вопросов теста, на которые он ответил правильно. На этом анализ результатов тестирования не закончен и мы продолжаем.

Пусть число правильных ответов b больше, чем m и мы отвергли гипотезу H_0. Это означает, что курсант знает правильный ответ хоть на один вопрос теста. Обозначим нижнюю границу числа вопросов, ответ на которые курсант знает символом s. Следовательно, $s = 1$.

Выдвинем новую пару гипотез, основную: H_0 – курсант знает правильный ответ только на один вопрос теста; и альтернативную: H_1 – курсант знает правильный ответ более чем на один вопрос теста.

Так как, в соответствии с основной гипотезой, курсант знает правильный ответ только на один вопрос теста, и на него он ответил правильно, уменьшим число вопросов теста в формуле на единицу, $n := n-1$. Также на единицу уменьшим число правильных ответов курсанта, $b := b-1$. Затем по формуле (3) найдем новое значение числа m и сопоставим с ним новое значение числа b.

Если новое значение b меньше или равно нового значения m, мы с той же самой доверительной вероятностью a можем утверждать, что новая гипотеза H_0 не противоречит результатам эксперимента, то есть курсант знает правильный ответ только на один вопрос теста. Все остальные правильные ответы им угаданы.

Если же новое значение b больше нового значения m, то мы с доверительной вероятностью a можем утверждать, что гипотеза H_0 неверна, верна альтернативная гипотеза H_1, и курсант знает правильный ответ более чем на один из вопросов теста, $s = 2$.

Во втором случае мы вновь уменьшаем на единицу величины n и b, по формуле (3) находим новое значение параметра m и выдвигаем новую пару гипотез:

– H_0 – курсант знает правильный ответ только на два вопроса теста;

– H_1 – курсант знает правильный ответ более чем на два вопроса теста.

Процесс итерационно продолжается до тех пор, пока n не окажется равным нулю, либо на очередной итерации гипотеза H_0 будет подтверждена.

В результате получим точное значение числа вопросов, ответ на которые курсант знает. Обозначим его символом S_0. Достоверность нашего вывода соответствует доверительной вероятности a.

Теперь нам известно число вопросов теста, ответы на которые курсант знает, при условии, что он правильно ответил на b вопросов и число вопросов – правильные ответы на которые он угадал. Следовательно, мы можем поставить курсанту за его знания объективную оценку, в соответствии с критериями, предложенными, например, в начале статьи.

Пример. Пусть тестируемому предъявлено шесть вопросов теста, $n = 6$. Каждый вопрос предполагает пять вариантов ответа, $\upsilon = 5$, только один из которых является правильным. Отсюда по формуле (1) получим $P_y = 0{,}2$. Тестируемый ответил правильно на три вопроса из шести, $b = 3$.

Найдем с помощью вышеописанной статистической модели ответы на то, сколько вопросов тестируемый знал, а сколько – угадал. Примем уровень значимости $a = 0{,}3$.

Шаг 1. В соответствии с формулой (3) получим $m = 2$. Поскольку $b > m$, в соответствии с формулой (5) приходим к выводу о том, что курсант *знал* ответ, по крайней мере, на один вопрос.

Шаг 2. В соответствии с моделью уменьшим на единицу параметры n и b.

Получим $n = 5, b = 2$. Отсюда по формуле по формуле (3) находим $m = 1$. Поскольку $b > m$, в соответствии с формулой (5) приходим к выводу о том, что курсант знал ответ, по крайней мере, на два вопроса.

Шаг 3. В соответствии с моделью уменьшим на единицу параметры n и b. Получим $n = 4, b = 1$. Отсюда по формуле (3) получим $m = 1$. Поскольку $b = m$, в соответствии с формулой (4) приходим к выводу о том, что курсант *угадал* ответ на третий вопрос.

Таким образом, курсант из трех правильных ответов знал ответы на два вопроса, а ответ на один вопрос угадал. Детальные расчеты для каждого из трех шагов приведены в таблице 1.

Таблица 1

Вспомогательные вычисления для примера

n	i					
	1	2	3	4	5	6
6	0,7379	0,3446	0,0998	0,0169	0,0016	0,00006
5	0,6723	0,2627	0,0579	0,0067	0,0003	–
4	0,5904	0,1808	0,0272	0,0016	–	–
3	0,488	0,104	0,008	–	–	–
2	0,36	0,04	–	–	–	–
1	0,2	–	–	–	–	–

Из таблицы 1 можно найти ответ на оставленный выше вопрос для любого уровня значимости. Так, для $x = 0{,}2$ получим следующие результаты. На первом шаге: $m = 2, b = 3$, на втором: $m = 2$, $b = 2$. Таким образом, для данного уровня значимости получим, что тестируемый знал правильный ответ только на один вопрос теста при двух угаданных ответах.

Для $x = 0{,}05$ на первом же шаге получим: $m = 3$. То есть для данного уровня значимости получим, что тестируемый все три правильных ответа на вопросы теста угадал. Поэтому выбор уровня значимости является исключительно ответственной задачей. На наш взгляд для оценки результатов тестирования достаточно уровня значимости $x = 0{,}3$. При таком уровне только каждый третий вывод о правильности гипотезы H_0 будет ошибочным.

Для проверки описанной выше статистической модели был проведен эксперимент. В ходе эксперимента были отобраны 20 курсантов.

Каждый курсант получил тест из шести вопросов. В каждом вопросе было пять вариантов ответа, только один из которых – правильный. Количество правильных ответов, данных курсантами в ходе тестирования, составляло от одного до четырех. З

адавшись уровнем значимости 0,3, с помощью нашей модели найдем количество вопросов, ответ на которые каждый курсант знал. Для тех курсантов, которые правильно ответили на четыре вопроса теста, получим следующие результаты.

На первом шаге: $m = 2$, $b = 4$; на втором: $m = 1$, $b = 3$; на третьем $m = 1$, $b = 2$; на четвертом $m = 1$, $b = 1$.

Таким образом, если тестируемый правильно ответил на 4 вопроса теста, то на самом деле он знал ответы на три вопроса, а ответ на один вопрос угадал.

Случай, когда курсант правильно ответил на три вопроса теста, разобран в вышеприведенном примере. Из примера следует, что курсант, правильно ответивший на три вопроса, знал ответы на два вопроса, а ответ на один – угадал.

Для тех курсантов, которые правильно ответили на два вопроса теста, на первом шаге получим: $m = 2$, $b = 2$; Это значит, что курсант не знал ответ ни на один вопрос и оба правильных ответа угадал.

Для тех курсантов, которые правильно ответили на один вопрос теста, на первом же шаге получим: $m = 2$, $b = 1$; Это значит, что курсант правильный ответ угадал.

Приведенные выше рассуждения в более компактном виде отображены в таблице 2.

Таблица 2

Вычисление параметра m для уровня значимости $a = 0{,}3$ и разных n, b

Номер шага вычислений	n	Количество правильных ответов							
		4		3		2		1	
		m	b	m	b	m	b	m	b
1	6	2	4	2	3	2	2	2	1
2	5	1	3	1	2	-	-	-	-
3	4	1	2	1	1	-	-	-	-
4	3	1	1	-	-	-	-	-	-
Количество угаданных ответов		1 из 4-х		1 из 3-х		2 из 2-х		1 из 1-го	

Результаты тестирования приведены в таблице 3.

Во втором и седьмом столбцах таблицы указано число правильных ответов курсантов.

В третьем и восьмом столбцах таблицы приведены оценки за правильные ответы. Средняя оценка по всем курсантам оказалась равной 3,75.

В четвертом и девятом столбцах приведены вычисленное по модели количество правильных ответов, данных курсантами вследствие знания этих ответов.

В пятом и десятом столбцах приведены оценки за правильные ответы, данные курсантами вследствие соответствующих знаний.

Средняя оценка по всем курсантам оказалась равной 3,0.

Таблица 3

Результаты тестирования курсантов при уровне значимости $\alpha = 0{,}3$

Номер курсанта по журналу учета	Число правильных ответов	Оценка за правильные ответы	Знал ответов	Оценка за знания	Номер курсанта по журналу учета	Число правильных ответов	Оценка за правильные ответы	Знал ответов	Оценка за знания
1	3	4	2	3	11	3	4	3	3
2	4	4	3	4	12	3	4	3	3
3	4	4	3	4	13	2	3	2	2
4	4	4	3	4	14	3	4	3	3
5	3	4	2	3	15	3	4	2	3
6	3	4	2	3	16	3	4	2	3
7	2	3	0	2	17	2	3	0	2
8	4	4	3	4	18	3	4	2	3
9	3	4	2	3	19	1	2	0	2
10	3	4	3	3	20	3	4	2	3

Столь существенной различие между средними баллами, полученными при традиционном методе оценки результатов тестирования и при предлагаемом методе, свидетельствует о том, что статистическая модель оценки результатов тестирования позволяет более объективно оценить степень усвоения курсантами учебного материала.

На практике тесты с числом вопросов равным шести не используются.

Здесь такой тест использовался только лишь для того, чтобы вычисления были разумными по объему.

Результаты исследований на тестах с числом вопросов двадцать и более позволяют сделать вывод о том, что в этом случае разница между средним баллом, рассчитанным при традиционном методе оценки результатов тестирования и при предлагаемом методе несколько снижается, однако все равно остается существенно выше статистической погрешности.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации».
2. Куватов В.И., Онов В.А., Яковлев Д.В. Технология формирования оптимальной последовательности изучения дисциплин учебного плана ВУЗа. Проблемы управления рисками в техносфере. 2012, Т.23, № 3, С.104–109.
3. Куватов В.И., Примакин А.И., Яковлев Д.В. Метод формирования оптимальной последовательности изучения модулей учебной дисциплины на основе кривых забывания. / Вестник Санкт-Петербургского университета МВД России. 2013, Т.58, № 2, С.172–178.
4. Примакин А.И. Универсальная система тестирования для организации мониторинга знаний учащихся в рамках дистанционно-модульной подготовки специалистов по информационной безопасности в учебных заведениях системы МВД России / Материалы VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011)». Санкт-Петербург, 26-28 октября 2011 г. \ СПОИСУ. – СПб., 2011, С.47–48.
5. Гмурман В.Е. Теория вероятностей и математическая статистика. – М.: Высшая школа, 2001, 480 с.
6. Свиридов А.П. Введение в статистическую теорию обучения и контроля знаний. Ч. 1. М.: МЭИ, 1974, 135 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СОЦИО-ТЕХНИЧЕСКИХ СИСТЕМ ЭКОНОМИЧНЫМИ СТРАТЕГИЯМИ УПРАВЛЕНИЯ ПОДГОТОВКОЙ ПЕРСОНАЛА

Залещанский Борис Данилович, Свиридов Александр Петрович, Павлова Ольга Александровна, Шалобина Елена Александровна,
Московский государственный технический университет радиотехники, электроники и автоматики,
Россия, Москва, Проспект Вернадского, д. 78,
e-mail: prof_sviridov@mail.ru, shalobina_olga@mail.ru, shalobina@mail.ru.

Аннотация: В статье рассмотрен подход к обеспечению качества подготовки персонала (обучаемых) для безопасного функционирования социо-технических систем на основе количественных характеристик динамики качества подготовки и экономических показателей.

Ключевые слова*: количественные характеристики; знания; умения; навыки.*

SECURITY SYSTEMS ECONOMICAL SOCIO-TECHNICAL TRAINING OF PERSONNEL MANAGEMENT STRATEGY

Zaleschansky Boris Danilovich, Sviridov Alexander, Olga Pavlova, Elena Shalobina,
Moscow State Institute of Radio Engineering, Electronics and Automation,
Russia, Moscow, Prospect Vernadskogo, d. 78,
e-mail: prof_sviridov@mail.ru, shalobina_olga@mail.ru, shalobina@mail.ru.

Abstract: The article describes the approach to quality assurance training (trainees) for the safe operation of socio-technical systems on the basis of the quantitative characteristics of the quality of training and economic indicators.

Keywords*: quantitative characteristics; knowledge; abilities; skills.*

Современные организации, предприятия и фирмы являются социо-техническими системами. Безопасность и эффективность их функционирования определяется не только техническими и программными средствами, но и деятельностью людей в их составе, уровнем знаний, умений, навыков и компетенций [1]. Отметим, что интенсивность отказа из-за ошибок персонала значительно превышает интенсивность отказа технических и программных средств [2].

В статье предлагается подход к обеспечению качества подготовки персонала (обучаемых) для безопасного функционирования социо-технических систем на основе количественных характеристик динамики качества подготовки и экономических показателей (затраты на обучение, контроль, потери из-за ошибочных действий персонала) [3,4].

Стратегия повторения или восстановления знаний в календарные моменты времени при известной функции распределения времени забывания

Периодические стратегии без учёта рисков недооценки и переоценки знаний. Повторения или восстановления знаний, умений, навыков и компетенций организуются следующим образом. Непосредственно после их усвоения через некоторый промежуток времени a планируется проведение контроля знаний и последующего повторения учебного материала (ПУМ). Если обучаемый (оператор) в течение этого промежутка времени не забывает учебный материал, то производится его повторение со средней длительностью Tw. В случае же забывания учебного материала до момента проверки организуется восстановление знаний со средней длительностью Te (Te > Tw). По завершении повторения или восстановления знаний, умений, навыков и компетенций планируется следующая проверка и повторение через интервал времени a и т.д.

При этом обучаемый (оператор) в произвольный момент времени может находиться в следующих состояниях знания:

E0 – состояние усвоения знаний, когда он может выполнить требуемые задачи, E1 – состояние необнаруженного (скрытого) забывания, E2 – состояние контроля и последующего восстановления знаний, E3 – состояние контроля и последующего повторения знаний.

Соответствующий граф переходов обучаемого (оператора) из одного состояния знания в другое приведен на рис. 1.

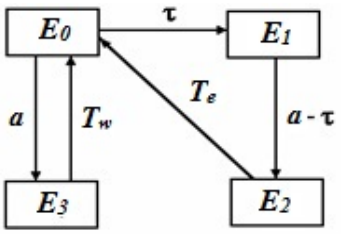


Рис. 1 Граф переходов обучаемого (оператора) из одного состояния знания в другое

На его основе можно получить соотношения для коэффициента профессиональной готовности K(a) обучаемого (оператора) и его максимума:

$$K(a) = \frac{\int_0^a [1 - F(x)]dx}{a + T_w + (T_e - T_w)F(a)} \quad (1)$$

$$K(a_0) = \max_a K(a) = \frac{1 - F(a_0)}{1 + (T_e - T_w)f(a_0)}. \quad (2)$$

где

$F(x)$ – функция распределения времени забывания,

a – интервал между проверками и повторениями,

T_w – время повторения,

T_e – время восстановления знаний.

Если время забывания имеет экспоненциальное распределение Exp(λ), то оптимальный интервал a_0 определяется в виде решения уравнения: dK(a)/da = 0 или

$$T_w = e^{\lambda^a} - 1 - \lambda a = g(\lambda a) \quad (3)$$

где

λ – интенсивность забывания.

Пример 1. Пусть для некоторого обучаемого (оператора) определено: λ=0,018 [1/мес.], Tw=8 [час], Te= 16 [час].

Определить оптимальный интервал между повторениями и максимальное значение коэффициента профессиональной готовности.

Решение. На рис. 2 приведена зависимость коэффициента профессиональной готовности от интервала между проверками: a0=108 [час], K(a0)=0,78.

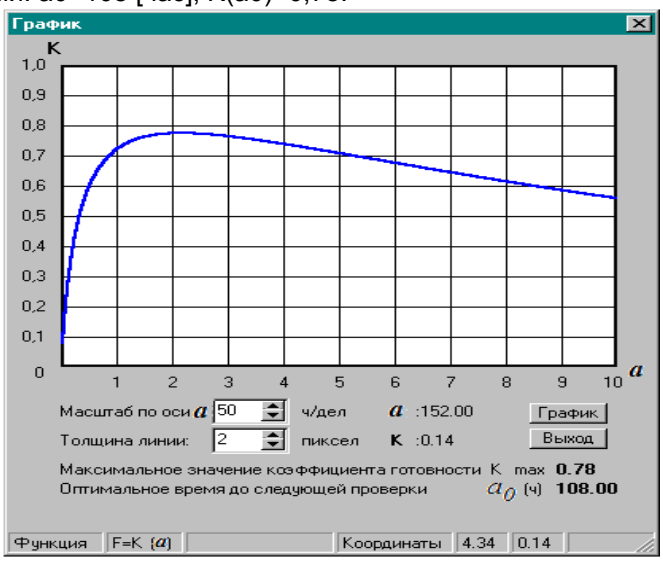


Рис. 2 Зависимость коэффициента профессиональной готовности от интервала между проверками

Учет затрат при управлении профессиональной готовностью

Пусть ci – затраты в единицу времени, когда обучаемый (оператор) находится в состоянии Ei, i=1,2,3. При этом средние удельные затраты C* равны (Свиридов, 1974, с. 88; Свиридов, 1981, с. 140; Süsse, Sviridov, 1998, с. 157; Свиридов, 2009, с. 284):

$$C^* = K^{-1} \sum_{i=1}^{3} c_i k_i \quad (4)$$

где: k_i – стационарная вероятность того, что обучаемый (оператор) находится в состоянии знаний E_i, i=1,2,3, а K – коэффициент профессиональной готовности. Подставив значения k_i и K в соотношение (4), получаем:

$$C^*(a) = \frac{C_1\int_0^a F(x)dx + c_3T_w + (c_2T_e - c_3T_w)F(a)}{\int_0^a [1 - F(x)]dx}.$$

Оптимальный интервал a_0, обращающий в минимум средние потери, определяется в виде решения уравнения $dC^*(a)/da=0$ или

$$\frac{c_3T_w}{c_2T_e - c_3T_w} = -F(a) + \lambda(a)\int_0^a\int[1 - F(x)]dx + \frac{C_1\int_0^a xdF(x)}{(c_2T_e - c_3T_w)F(a)} \qquad (5)$$

Минимум средних удельных затрат при этом равен:

$$\min_a C^*(a) = C^*(a_0) = C_1\frac{F(a_0)}{1-F(a_0)} + \lambda(a_0)(c_2T_e - c_3T_w).$$

Если время забывания имеет экспоненциальное распределение Exp(λ), то из уравнения (5) следует:

$$\frac{C_3}{C_1}\lambda T_w = e^{\lambda a} - 1 - \lambda a = g(\lambda a). \qquad (6)$$

Пример 2. Дано: λ=0,0015 [час-1], Tw=8 [час], Te=16 [час], c1=2, c2=2, c3=1.

Определить: 1) оптимальный интервал a0 между проверками и повторениям или восстановлениями знаний и 2) минимум средних потерь C(a0).

Решение. На рис. 3 приведена зависимость C(a) средних удельных потерь от интервала между проверками: a0=72 [час], Cmin=C(a0)=0,26.

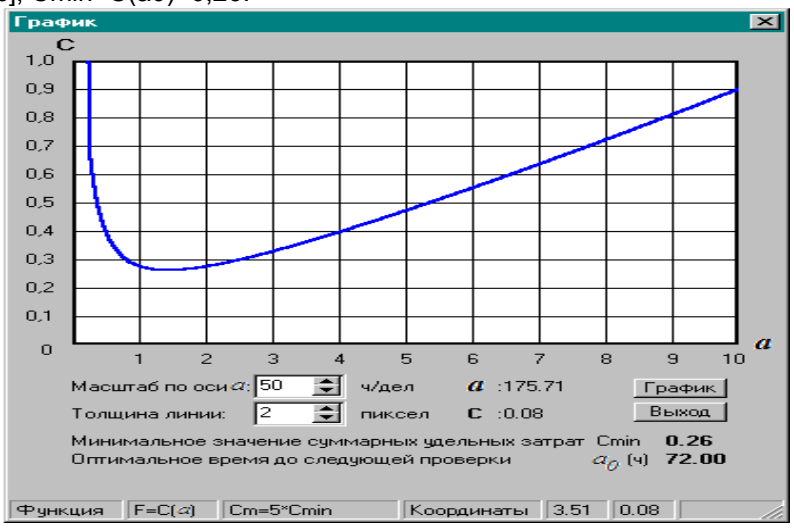


Рис. 3 Зависимость средних удельных потерь от интервала между проверками

Строго периодическое повторение или восстановление знаний при учете рисков недооценки и переоценки знаний

Повторения и восстановления знаний организуются подобно предыдущей стратегии. Непосредственно после усвоения учебного материала через промежуток времени a планируется проверка знаний. Если контроль проводится с помощью компьютерной системы, то следует учитывать риски недооценки и переоценки знаний α и β. Средняя длительность проверки знаний равна tk.

Если обучаемый (оператор) сохраняет знания до момента проверки, то при проверке знаний он с вероятностью (риск недооценки) α получает неудовлетворительную оценку. При этом ему предлагается восстановить знания. Средняя длительность восстановления знаний равна te (te > tk). С вероятностью (1-α) он получает заслуженную положительную оценку. В этом случае производится повторение учебного материала.

Если обучаемый (оператор) забывает учебный материал до момента проверки знаний, то с вероятностью (1-β) он получает заслуженную неудовлетворительную оценку. При этом ему предлагается восстановить знания. С вероятностью (риск переоценки) β он получает незаслуженную удовлетворительную оценку.

В произвольный момент времени обучаемый (оператор) может находиться в следующих состояниях:

E0 – состояние усвоения знаний, когда он может выполнить требуемые задачи, E1 – состояние необнаруженного (скрытого) забывания, E2 – проверка обучаемого (оператора), забывшего учебный материал, E3 – состояние восстановления знаний, умений или навыков, E4 – проверка знаний обучаемого (оператора), не забывшего учебный материал, E5 – состояние скрытого забывания, необнаруженного в результате риска переоценки при контроле знаний.

Матрица вероятностей перехода из одного состояния знаний в другое имеет вид:

$$\mathbf{P}(a)=\begin{pmatrix} 0 & F(a) & 0 & 0 & 1-F(a) & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-\beta & 0 & \beta \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1-\alpha & 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Граф переходов обучаемого (оператора) из одного состояния знаний в другое приведен на рис. 4.

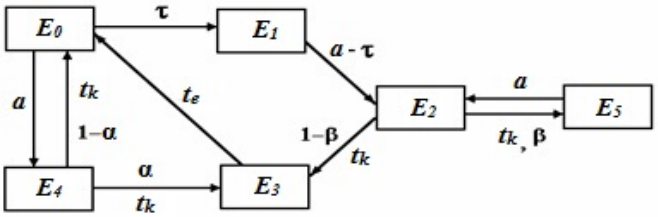


Рис. 4 Граф переходов обучаемого (оператора) из одного состояния в другое при контроле знаний с рисками недооценки и переоценки знаний

Динамика знаний обучаемого (оператора) описывается при этом полумарковским процессом. Коэффициент профессиональной готовности обучаемого равен (Свиридов, 1981, с. 177):

$$K(a)=\frac{\int_0^a [1-F(t)]dt}{(a+t_k)(1+\frac{\beta F(a)}{1-\beta})+t_e(1-\beta)[F(a)+\alpha(1-F(a))]} \qquad (7)$$

Если время забывания имеет экспоненциальное распределение Exp(λ), то из соотношения (7) следует:

$$K(a)=\frac{(1-\beta)(1-e^{-\lambda a})}{\lambda\{(a+t_k)(1-\beta e^{-\lambda a})+\lambda t_e(1-\beta)^2[1-(1-\alpha)e^{-\lambda a}]\}}. \qquad (8)$$

Оптимальный интервал между проверками и повторениями знаний можно определить по максимуму коэффициента профессиональной готовности (7) или (8).

Пример 3. Применим рассмотренную стратегию к операторам сложной и ответственной системы. Для них определены характеристики динамики знаний: интенсивность забывания λ=0,05-0,40 [1/мес.], математическое ожидание времени восстановления знаний te=3 час, математическое ожидание времени контроля знаний tk=0,5 час.

Предположим, что контроль знаний проводится с помощью компьютерной обучающей системы с риском недооценки α=0,35 и переоценки знаний β=0,40. Необходимо определить оптимальные интервалы между проверками и повторениями знаний. Практический интерес представляет также решение следующей задачи: как влияют отклонения от оптимального значения интервала между проверками и повторениями знаний на коэффициент профессиональной готовности обучаемого (оператора)?

Решение. В табл.1 приведены оптимальные значения a0 и максимумы коэффициента профессиональной готовности K(a), а также значения коэффициента профессиональной готовности K(a) при проведении контроля знаний через интервал времени a=600 час.

Таблица 1

Характеристики	λ[1/мес.]					
	0,05	0,10	0,15	0,20	0,30	0,40
$K_{max}=K(a_0)$	0,98	0,97	0,96	0,955	0,945	0,94
a_0 в час	160	100	80	70	60	50
K(a=600 час)	0,95	0,91	0,87	0,83	0,76	0,71

Из таблицы следует, что оптимальный интервал a_0 для операторов с интенсивностью забывания λ=0,05 [1/мес.] составляет 160 час (примерно 7 дней), а для оператора с λ=0,40 [1/мес.] - a_0=50 час (примерно 2 дня).

Если контроль знаний оператора с λ=0,40 [1/мес.] вместо оптимального интервала a_0=50 час проводится через интервал a=600 час, то коэффициент профессиональной готовности снижается с 0,94 до 0,71. Этот пример показывает влияние отклонений от оптимального значения интервала между проверками и повторениями знаний на коэффициент профессиональной готовности обучаемого (оператора).

СПИСОК ЛИТЕРАТУРЫ

1. Проблемы подготовки кадров в сфере инфокоммуникационных технологий, Санкт-Петербургская научно-практическая конференция, Санкт-Петербург, 1-3 марта 2005 г.: Материалы конференции. – СПб.: СПОИСУ, 2005. – 156 с.
2. Сальвенди Г. (1991): Человеческий фактор (Handboock of Human Factors). – М.: Мир.
3. Свиридов А.П. (1981): Основы статистической теории обучения и контроля знаний. – М.: Высшая школа.
4. Свиридов А.П. (2009): Статистическая теория обучения. Монография. – М.: РГСУ.

УДК 378.147
ГРНТИ 14.07.09

ПРИМЕНЕНИЕ МОДУЛЬНОГО ПРИНЦИПА, КАК ФОРМЫ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ПОДГОТОВКЕ КУРСАНТОВ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 090915.65 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ»

Куватов Валерий Ильич[1], Примакин Алексей Иванович[1], Синещук Юрий Иванович[2],
[1]Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
[2]Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия»,
Россия, Санкт-Петербург, Петродворец, улица Разводная, д. 15,
e-mails: kyb.valery@yandex.ru, a.primakin@mail.ru, sinegal@rambler.ru.

Аннотация: Статья посвящена применению блочно-модульных технологий при построении образовательных стандартов, учебных планов и образовательных программ с целью повышения эффективности подготовки курсантов Санкт-Петербургского университета МВД России по специальностям технической направленности. Модульный подход способствует индивидуализации образовательных программ, позволяет устанавливать темп и время их освоения, своевременно выявлять пробелы в знаниях и понимании учебного материала каждым учащимся.

Ключевые слова: *блочно-модульные технологии; модуль; образовательные стандарты; дисциплины учебного плана; компетенция; компетентностный подход.*

APPLICATION OF THE MODULAR PRINCIPLE AS FORMS OF THE ORGANIZATION OF EDUCATIONAL ACTIVITY WHEN TRAINING CADETS OF THE MINISTRY OF INTERNAL AFFAIRS ST. PETERSBURG UNIVERSITY OF RUSSIA IN THE SPECIALTY 090915.65 – «SAFETY OF INFORMATION TECHNOLOGIES IN THE LAW-ENFORCEMENT SPHERE»

Kuvatov Valery Ilyich[1], Primakin Alexey Ivanovich[1], Sineshchuk Yury Ivanovich[2],
[1]Ministry of Internal Affairs 1sankt-Peterburgsky university of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
[2]Voyenny educational scientific center of Navy «Naval academy»,
Russia, St. Petersburg, Petrodvorets, Razvodnaya Street, 15,
e-mails: kyb .valery@yandex.ru, a.primakin@mail.ru, sinegal@rambler.ru.

Abstract: Article is devoted to application of block and modular technologies at creation of educational standards, curricula and educational programs for the purpose of increase of efficiency of training of cadets of the Ministry of Internal Affairs St. Petersburg university of Russia for specialties of a technical orientation. Modular approach promotes an individualization of educational programs, allows to establish speed and time of their development, in due time to reveal gaps in knowledge and understanding of a training material each pupil.

Keywords: *block and modular technologies; module, educational standards; disciplines of the curriculum; competence; competence-based approach.*

В соответствии со статьей 13 «Общие требования к реализации образовательных программ» Федерального закона 273-ФЗ РФ «Об образовании в Российской Федерации», вступившего в силу с 1 сентября 2013 года, указывается: «При реализации образовательных программ организацией,

осуществляющей образовательную деятельность, может применяться форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании соответствующих образовательных технологий» [1].

Открытие и осуществление первого набора курсантов в Санкт-Петербургском университете МВД России по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере» предполагает применение, отмеченной в Законе, педагогической технологии – модульного принципа.

Кафедра специальных информационных технологий, являющаяся выпускающей кафедрой по указанной выше специальности, вносит свои предложения по оптимизации рабочего учебного плана специальности 090915.65 с применением блочно-модульных технологий [2], разрабатывает методы формирования оптимальной последовательности изучения модулей учебных дисциплин на основе кривых забывания [3].

Модульная организация построения основной образовательной программы (ООП) тесно связано с инновационным образованием. Традиционная организация учебного процесса в виде семестров и экзаменационных сессий нередко приводит к низкому качеству освоения образовательных программ, поскольку их интенсивное изучение бывает отнесено на период зачётных и экзаменационных сессий, а систематическая работа в семестре фактически отсутствует. За время сессий, чаще всего, обучающийся просто не в состоянии глубоко разобраться в учебном материале [4].

Причинами, приведшими к использованию блочно-модульных технологий в построении образовательных стандартов, учебных планов и образовательных программ являются:

– повышение гибкости образовательных программ;

– облегчение определения «точек» входа и «точек» выхода курсанта в его индивидуальной образовательной траектории;

– необходимость увязки всех компетенций к конкретным дисциплинам, практикам, модулям и циклам (вместе с тем, необходимо отметить, что существует некоторое подмножество компетенций, которое формируется самой средой образовательной организации в период пребывания в ней обучающегося);

– минимизация трудозатрат при оперативной модификации различных видов модулей, включаемых в учебные дисциплины, внесение новых или удаление устаревших модулей, в соответствии с требованиями ФГОС ВПО «высшие учебные заведения должны ежегодно обновлять основные образовательные программы с учетом развития науки, культуры, экономики, техники, технологий и социальной сферы»;

– необходимость реализации требований о текущем контроле и обеспечении оценки достижений обучаемых с учетом системности работы;

– возможность оперативно формировать содержательно новые курсы из модулей, как части одно-, или много-семестровой дисциплины;

– необходимость реализации концепции непрерывного образования и связанные с ней программы повышения квалификации и переподготовки специалистов также требуют более компактных, но информативных и логически завершённых дидактических единиц со своей достаточно совершенной системой контроля знаний обучающихся, чем и являются модули семестровой дисциплины.

Поэтому можно утверждать, что блочно-модульное построение учебных планов и образовательных программ учебных дисциплин является одним из основных принципов развития образования и повышения эффективности подготовки специалистов, в том числе, по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере».

Вместе с тем, из триады, характеризующей инновационный характер нового поколения образовательных стандартов: компетенция – модуль – зачетная единица, понятие модуля наименее методически разработано и наиболее сложно для понимания, по нему не выработано достаточно согласованных документов.

В отечественной и иностранной литературе можно встретить различное понимание понятия «модуль», даже в такой достаточно узкой сфере, как организация учебного процесса: модуль обучения, учебный модуль, предметный модуль, программный модуль и т. п. Понятие «модуль» трактуется по-разному – от совокупности дисциплин, объединенных в общий модуль (цикл) на базе их логической и методической связи, до модуля, являющегося частью дисциплины. Понятие «Модуль» описано в документах Болонского процесса: завершенная с точки зрения результатов обучения часть программы, имеющая четко сформулированные результаты и критерии оценки. В высшем образовании модуль чаще всего реализуется в течение одного семестра [5].

Поэтому при разработке ООП и рабочих программ учебных дисциплин целесообразно использовать модульную организацию дисциплин, как элемента кредитно-модульной организации учебного процесса, ориентированного на компетентностный подход, применяемый в ГОС ВПО третьего поколения [6], определяя, при этом, модуль – как часть учебной дисциплины или

совокупность учебных дисциплин, имеющая наименование и определённую логическую завершённость по отношению к установленным целям и результатам обучения (в том числе к сформированным компетенциям) и завершающаяся промежуточной аттестацией (или – для части учебной дисциплины – текущим контролем успеваемости).

Целью разработки модулей, как составных частей дисциплины, можно считать [7]:

1. Расчленение содержания дисциплины на логически завершенные части, отвечающие профессиональным, педагогическим и дидактическим задачам, определение для всех частей дисциплины целесообразных видов и форм обучения для повышения качества преподавания и восприятия учебного материала.

2. Анализ совокупности полученных модулей всех дисциплин образовательной программы на отсутствие содержательного дублирования, временных и логических разрывов между модулями различных дисциплин, видами и формами обучения, усиление междисциплинарных связей.

3. Повышение эффективности самостоятельной работы учащихся путём улучшения её организации и усиления текущего контроля.

Достижение сформулированных целей предполагает удовлетворение следующих требований:

Семантическая самостоятельность – подразумевает чёткие контуры предмета изучения. Любой модуль должен включать самостоятельную часть учебной информации, каждая единица которой измеряется и оценивается, для чего разрабатываются материалы для самоконтроля и текущего контроля.

Самодостаточность – предполагает, что модуль содержит только необходимые и достаточные сведения, позволяющие полностью раскрыть содержание изучаемой часть учебной информации.

Реализация этих требований может быть обеспечена соблюдением основных принципов модульного обучения, к которым относятся:

1. Системный подход к построению структуры дисциплины, самих образовательно-профессиональных (основных и дополнительных) программ и определению их содержания;

2. Структурирование знаний на обособленные элементы, проблемность учебного материала, формирующая осознанную перспективу интеллектуального роста, и ясно выраженный принцип сотрудничества обучающих и обучающихся.

3. Обеспечение методически правильного согласования всех видов учебных занятий внутри каждого модуля и между ними.

4. Гибкость структуры построения модульного курса и самих образовательных программ, возможность оперативного формирования содержательно новых курсов.

5. Эффективный контроль знаний обучающихся, рассредоточение по семестру (периоду обучения) контрольных мероприятий.

6. Возможность индивидуализации обучения и установления индивидуальных рейтингов обучающихся.

7. Возможность реализации методических принципов развивающего обучения, при которых создаются предпосылки для творческой деятельности обучающихся.

Кроме этого, в основе методики формирования модулей, а так же последовательности изучения их курсантами лежат следующие положения.

Все дисциплины учебного плана можно поделить на группы взаимосвязанных дисциплин или модулей. Существует три типа отношений между дисциплинами (модулями) учебного плана: отношения следования, отношения взаимной независимости и отношения взаимной зависимости.

Если две дисциплины (модули) связаны отношением следования, то изучение одной из них можно начинать только после окончания изучения другой дисциплины (или определенных тем другой дисциплины). Так, например, изучению физики должно предшествовать изучение определенных разделов математики.

Если между двумя дисциплинами существует отношение взаимной независимости, то их изучение может вестись произвольно по отношению друг к другу, в том числе, они могут изучаться параллельно. Так, например, взаимно независимыми являются дисциплины информатика и история.

Последний, третий тип отношений означает, что изучение дисциплин должно вестись параллельно, с учетом зависимости между темами. Такое отношение встречается редко, как правило, оно свидетельствует о том, что деление области знаний между дисциплинами проведено неверно. Поэтому мы взаимную зависимость между дисциплинами учитывать не будем.

Одно из важнейших свойств памяти человека – ассоциативность. В группе из двух дисциплин связанных отношением следования, чем больше ассоциаций возникает у курсантов при изучении последующей дисциплины, тем эффективнее ее изучение. Другое важнейшее свойство памяти – забывание. Если временной интервал между дисциплинами, связанными отношениями следования

велик, то большая часть предшествующей дисциплины забыта и количество ассоциаций, возникающих у курсантов при изучении последующей дисциплины меньше. Поэтому, учебный план тем оптимальнее, чем меньше временные интервалы между дисциплинами (модулями) связанными отношением следования.

Применение модульного принципа, как формы организации образовательной деятельности, позволило оптимизировать учебные планы и повысить эффективность подготовки курсантов по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере» в Санкт-Петербургском университете МВД России [8].

Таким образом, модульный подход способствует индивидуализации образовательных программ, позволяет устанавливать темп и время их освоения, своевременно выявлять пробелы в знаниях и понимании учебного материала каждым обучающимся.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации».
2. Куватов В.И., Пантиховский О.В., Примакин А.И., Синещук Ю.И. Применение блочно-модульных технологий для оптимизации учебных планов и повышения эффективности подготовки курсантов по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере» / Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013, С.236–237.
3. Куватов В.И., Примакин А.И., Яковлев Д.В. Метод формирования оптимальной последовательности изучения модулей учебной дисциплины на основе кривых забывания / Вестник Санкт-Петербургского университета МВД России, №2 (58), 2013, С.172–178.
4. Сенашенко В.С. О соотношении зачетных единиц и модульной структуры учебного процесса. // Информационный бюллетень. №6, УМО в области инновационных междисциплинарных образовательных программ. СПб., 2005.
5. http://fgosvpo.ru/uploadfiles/mo/20111108182212.pdf (из «Глоссарий Болонского процесса»).
6. Психолого-педагогическое сопровождение реализации инновационных образовательных программ / Под ред. Ю.П. Зинченко, И.А. Володарской. – М.: Изд-во МГУ, Серия «Инновационный Университет», 2007, 120 с.
7. Общее представление о модулях в области организации образовательного процесса. Причины использования модульного подхода Ю.Б. Васенёв. http://www.umu.spbu.ru/
8. Куватов В.И., Пантиховский О.В., Синещук Ю.И. Применение блочно-модульных технологий для оптимизации учебных планов и повышения эффективности подготовки курсантов по специальности 090915.65 – «Безопасность информационных технологий в правоохранительной сфере» / Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013, С.236-237.

СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ – ИННОВАЦИОННОЕ НАПРАВЛЕНИЕ ИССЛЕДОВАНИЙ И ПОДГОТОВКИ СПЕ-ЦИАЛИСТОВ ИТ

Пуха Геннадий Пантелеевич,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21,
e-mail: pgp2003@list.ru.

Аннотация: в статье обосновываются актуальность научных исследований в области систем интеллектуальной поддержки принятия решений, методология их формирования и целесообразность открытия соответствующей магистерской программы ВПО.

Ключевые слова: *предприятие; управление; решение; интеллектуальная поддержка; программное обеспечение; методология формирования разработки; магистерская программа*

SYSTEMS OF INTELLECTUAL SUPPORT DECISION MAKING — INNOVATION DI-RECTION OF THE STUDIES AND PREPARATION IT-SPECIALISTS

Pooha Gennady Panteleevich,
Saint-Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21.
e-mail: pgp2003@list.ru.

Abstract: in article are motivated urgency of the scientific studies in the field of systems of knowledge-based support decision making, methodology of their shaping and practicability of the opening corresponding to magistracy of the program of the high vocational training.

Keyword: *enterprise; control; decision; knowledge-based support decision; software; methodology of the shaping the development; magistracy program*.

1) Современное развитие ЭВТ обеспечило широкие возможности для создания и успешного использования средств обработки данных различного назначения, а, поэтому, одним из актуальных направлений развития современных информационных технологий становится разработка, так

называемых, систем интеллектуальной поддержки принятия решения (СИП ПР) в органах управления (ОУ) предприятиями [1].

Согласно, например [2], системы поддержки принятия решения (СППР) представляют собой системы, максимально приспособленные к решению задач повседневной управленческой деятельности, являются инструментом, призванным оказать помощь лицам, принимающим решения (ЛПР).

СППР, как правило, являются результатом мультидисциплинарного исследования, включающего теории баз данных, искусственного интеллекта, интерактивных компьютерных систем, методов имитационного моделирования, обеспечивающих выбор решений некоторых неструктурированных и слабоструктурированных задач, в том числе и многокритериальных.

Ранние определения СППР (в начале 70-х годов прошлого века) отражали следующие три момента: (1) возможность оперировать с неструктурированными или слабоструктурированными задачами, в отличие от задач, с которыми имеет дело исследование операций; (2) интерактивные автоматизированные (то есть реализованные на базе компьютера) системы; (3) разделение данных и моделей. Следовательно — совокупность процедур по обработке данных и суждений, помогающих руководителю в принятии решений, основанная на использовании моделей [3], может служить, на наш взгляд, наиболее общим определением СППР.

В настоящее время нет общепринятого определения СППР, поскольку конструкция СППР существенно зависит от вида задач, для решения которых она разрабатывается, от доступных данных, информации и знаний, а также от пользователей системы. Тем не менее, можно привести некоторые элементы и характеристики, общепризнанные, как части СППР.

Так, в большинстве случаев СППР — это интерактивная автоматизированная система, которая помогает ЛПР использовать данные и модели для идентификации и решения задач и принятия решений. Система должна обладать возможностью работать с интерактивными запросами с достаточно простым для изучения языком запросов.

Согласно Turban [3], СППР обладает следующими четырьмя основными характеристиками:

– СППР использует и данные, и модели;
– СППР предназначены для помощи менеджерам в принятии решений для слабоструктурированных и неструктурированных задач;
– они поддерживают, а не заменяют, выработку решений менеджерами;
– цель СППР — улучшение эффективности решений.

В связи с изложенным выше, мы также, под средствами такого класса будем понимать, определенную совокупность программного обеспечения для информационных и расчетных задач, решение которых с помощью ЭВМ обеспечивает разработку наиболее целесообразных планов производства или выработку рациональных вариантов управления предприятием, как в обычной обстановке, так и в кризисной ситуации.

Актуальность разработки и применения подобных систем очевидна. С одной стороны, она обуславливается слишком высокой «ценой» не обосновано принятых, например, экономических решений, а, с другой - сложностью такого обоснования без соответствующих вспомогательных средств.

В то же время, состояние дел в указанном направлении развития современных информационных технологий, особенно в области разработки СППР для ОУ предприятиями сферы сервиса, нельзя признать удовлетворительным, даже несмотря на появление многочисленных поисковых информационных систем (ИС), создаваемых на основе технологии баз данных.

Дело в том, что методология проектирования поисковых ИС уже имеет серьезный теоретический базис и развитые инструментальные средства для их разработки. Возникла целая индустрия программного обеспечения СУБД, которая особенно активно развивается в области персональных ЭВМ. Благодаря чему появилась возможность сравнительно легкого изготовления, в том числе и с привлечением web-технологий, простых прикладных средств простой информационной поддержки управленческих процессов, связанных с организацией документооборота как ключевого звена в организации финансового и управленческого учета на предприятии.

Именно этот благоприятный в целом фактор и имеет неожиданные негативные последствия - формирует неполное представление о структуре и характере СППР П как об обычном структурированном наборе сведений о производственном процессе и средств, обеспечивающих реализацию рекламных мероприятий и автоматизированного документооборота [4].

Подобные трактовки информационной поддержки принятия решения в рассматриваемом направлении развития ИТ далеко не безобидны, так как именно они являются, на наш взгляд, основными причинами, сдерживающими его развитие. Поэтому без серьезных методологических проработок наиболее целесообразного построения и условий успешной разработки ПО этого класса, даже в условиях приличного финансирования, существенных результатов в создании СППР ожидать достаточно проблематично.

В связи с этим, возникает необходимость исследовать вопрос о формировании СППР и технологиях их реализаций именно с методологических позиций.

2) Как известно, независимо от уровня (или звена) основными функциями управления являются: планирование, учет, анализ и регулирование.

Очевидно, что все эти функции, в той или иной степени, связаны с основными операциями по обработке данных (сбор, формализация, фильтрация, защита, транспортировка и преобразование) в интересах получения новых сведений (информации) о состоянии управляемого объекта и выработки новых управляющих воздействий. Поэтому с точки зрения реализации этих функций, процесс управления носит явно выраженный информационный характер (рис. 1).

Рис. 1. Состав системы управления

В связи с данным обстоятельством, в структуре любой системы управления может быть выделен такой реально существующий функциональный элемент, назначение которого состоит в том, чтобы по результатам обработки имеемых данных обеспечить поддержку принятия органами управления наиболее целесообразных решений [5]. В качестве такого функционального элемента систем управления чаще всего определяют так называемые информационные подсистемы или информационные системы (ИС) в случае их рассмотрения как самостоятельного объекта.

При этом очевидно, что функционирование ИС обеспечивается всеми подсистемами системы управления, а результаты ее работы используется подсистемой органов управления в интересах наиболее эффективного воздействия на управляемый объект.

Исходя из назначения ИС, которая, как уже отмечалось выше, должна претендовать на решение задачи по обеспечению поддержки принятия органами управления наиболее целесообразных решений за счет анализа результатов обработки данных о состоянии управляемого объекта, естественно предположить, что в качестве основных элементов ИС должны выступать (рис. 2):

– комплекс (набор) расчетно-аналитических задач, позволяющий производить оценку эффективности принимаемых решений по результатам функционирования объекта управления;

– банк (или база) данных (или знаний), соответствующая предметной области применения ИС;

– программно-аппаратный интерфейс пользователя, обеспечивающий функционирование элементов ИС как единого целого и удобство их использования.

Рис. 2. Состав программных средств интеллектуальной поддержки принятия решений

Действительно, исследования процессов принятия решений при управлении в различных сферах человеческой деятельности показывают, что их обоснованность напрямую зависит от корректности той методологии, которая заложена в основу оценки эффективности функционирования объекта управления, а также - выработки целесообразного варианта корректирующих его поведение воздействий, и реализована в соответствующих расчетных методиках [6].

В связи с этим необходимо иметь в виду, что научная проблема, связанная с разработкой СППР в той или иной области состоит, обычно, не столько в том, как строить их программные средства, а, сколько в том - как оценивать эффективность работы управляемого объекта и как вырабатывать оптимальное решение на изменение его состояния.

Таким образом, необходимо признать, что самым важным условием (методологическим принципом) успешного формирования и функционирования СППР, в том числе и для предприятий сферы сервиса, является, прежде всего, наличие в их основе комплекса специальных расчетных задач, обеспечивающих анализ (хотя бы) и (еще лучше) синтез структуры управляемого объекта. При этом также очевидно, что все эти задачи должны быть подчинены единой цели их решения, которая предполагает либо определение выбранного показателя эффективности в случае анализа объекта, либо нахождение экстремума показателя эффективности при оптимизации процесса работы объекта. Кроме этого, требуется установить взаимосвязи между частными задачами, по соответствующим показателям и согласовать их по входным и выходным параметрам.

3) Как и к любому материальному объекту с ИС можно применить ту или иную систему классификации.

Так, например, в зависимости от степени их интеллектуализации (реализации мыслительных возможностей деятельности человека) ИС целесообразно подразделить на следующие классы [5].

– информационно-поисковые системы (ИПС), в которых отсутствуют элементы и задачи анализа;

– интеллектуальные ИС (ИИС), обеспечивающие обработку данных в интересах решения задач анализа и (или) синтеза объектов определенной предметной области, а также

– экспертные ИС (ЭИС)– основанные на базах знаний и соответствующих методов работы с ними.

Системы перечисленных классов, реализованные в той или иной степени в виде программных продуктов, уже давно находят свое естественное применение, в области организации управления различными сложными системами [10].

а) Несомненно, что наибольшее распространение получили ИПС, обеспечивающие поиск и отбор необходимых данных в специальных базах с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска. При этом их главной задачей является поиск информации релевантной информационным потребностям пользователя (релевантность - это соответствие результатов поиска сформулированному запросу). В связи с этим основными показателями ИПС являются пространственный масштаб и специализация. Так, по пространственному масштабу ИПС можно разделить на локальные, глобальные, региональные.

б) В пользу выделения по данному признаку отдельного класса интеллектуальных ИС (ИИС) говорит факт существования целого спектра прикладных программных средств типа: ERP, GIS, DocFlow, Business Modeller, SCADA/ DCE, Project Management и др., которые по своему функциональному назначению можно отнести к системам поддержки принятия решений — как минимум на 50% они для этого и создавались. Они, в отличие от ИПС, уже предназначаются именно для помощи лицу, принимающему решения, в использовании связей, данных, документов, знаний и моделей для идентификации и решения проблем и формирования решений.

Так, например [7], ERP-система — конкретный программный пакет, реализующий организационную стратегию интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия (Enterprise Resource Planning — планирование ресурсов предприятия).

К этому же классу систем тяготеют, на наш взгляд, и так называемые инструментальные средства бизнес-интеллекта (Business Intelligence Tools) — программное обеспечение, которое дает возможность пользователям наблюдать и использовать большие объемы сложных данных.

Ну и, наконец, группа прикладных программных средств, предназначение которых «поддержка принятия решений», с одной стороны, декларируется напрямую в их названии — Decision Support Systems (DSS), а с другой — это предназначение до сих пор трактуется, к сожалению, по-разному.

Не будем здесь приводить все встречающиеся определения данной группы прикладного ПО, укажем лишь, что из всех вариантов наиболее подходящими, по-нашему мнению, являются те, в которых отмечается не только возможность «манипуляции данными», но и «построения и использования математических моделей», а также — аппарата «искусственного интеллекта». Именно использования математических методов и моделей в интересах решения задач анализа процессов и систем в определенной предметной области и (или) синтеза рациональных вариантов их построения и управления ими, должны быть отличительным признаком для класса интеллектуальных ИС, претендующих в то же время на «высокое звание» СППР.

в) В некоторых определениях упоминается также возможность включения в состав DSS-системы функциональных возможностей искусственного интеллекта. Подобным разновидностям

программных средств этой группы найдется местечко как раз в классе *экспертных* ИС, которые должны иметь «звание» интеллектуальных СППР более высокого уровня.

Как известно [9], в информатике экспертные системы рассматриваются совместно с базами знаний как модели поведения экспертов в определенной области знаний с использованием процедур логического вывода и принятия решений, а базы знаний — как совокупность фактов и правил логического вывода в выбранной предметной области деятельности.

Таким образом, выделение группы ИС, перед которыми в рамках определенных предметных областей стоит задача анализа и синтеза процессов на основе методов математического моделирования в интересах формирования рациональных вариантов их организации (построения систем) или управления ими, в отдельный класс интеллектуальных ИС (Decision of Intellectual Support System - DISS) — является объективной необходимостью.

В то же время, ИИС, совместно с классом экспертных ИС, принципы построения и функционирования которых основаны на методах экспертных оценок и обработке баз знаний, а предназначением также является анализ и синтез управленческих процессов, и составляют по существу вид прикладного ПО под общим названием системы поддержки принятия решений – СППР (таблица 1.1).

Таблица 1.1

<table>
<tr><th colspan="3">ИС</th></tr>
<tr><th>ИПС:</th><th>ИИС:</th><th>ЭИС:</th></tr>
<tr><td>Локальные</td><td>Планирование ресурсов предприятия – ERP и им подобные</td><td>статические</td></tr>
<tr><td>Региональные</td><td rowspan="2">Инструментальные средства бизнес-интеллекта (Business Intelligence Tools):
➢ средства многомерного анализа (On-Line Analytical Processing –OLAP);
➢ инструментальные средства запросов (Query Tools);
➢ инструментальные средства поиска данных (Data Mining Tools)</td><td>квазидинамически</td></tr>
<tr><td rowspan="3">Глобальные
➢ каталоги;
➢ поисковые системы;
➢ метапоисковые системы.</td><td>динамические</td></tr>
<tr><td></td><td>интерпретации данных, диагностирования, мониторинга, проектирования, прогнозирования, сводного планирования, обучения, управления, ремонта и отладки.</td></tr>
<tr><td></td><td colspan="2">Системы поддержки принятия решений (СППР)
Decision Support Systems (DSS)</td></tr>
</table>

На основании анализа уже сложившейся практики в качестве предмета для систем класса DSS в области бизнеса чаще всего выступают: финансовый анализ и прогнозирование; маркетинг реализации и закупок; анализ стереотипов клиентского поведения и выявление скрытых закономерностей; анализ рисков; управление активами.

В более крупном масштабе можно говорить о том, что информационные технологии сосредоточены на обслуживании процессов, связанных с: людьми, процессами, стратегиями и технологиями.

Из этого следует, что в сферу приложения систем DSS попадает почти половина структурных задач, возлагаемых на ИТ-службы. Данное обстоятельство находит подтверждение при анализе рынка прикладных информационных систем. Так, мировой рынок, например, ERP-систем оценивается в настоящее время оборотами порядка 25 млрд. долларов. Рынок DSS-систем, который возник только в середине 90-х годов, сейчас оценивается суммой порядка 10 млрд. долларов и растет существенно большими темпами, чем рынок корпоративных систем управления. Его рост порядка 30% в год против 10-15% роста ERP-рынка, и можно предположить, что в течение ближайших пяти лет можно ожидать достижения паритета.

С другой стороны, если рынок систем DSS в настоящее время в основном связан с финансовым сектором, крупноформатной торговлей и телекоммуникациями, то можно ожидать постепенной ассимиляции функциональных возможностей DSS-систем в существующие системы ERP-класса, что, по-видимому, приведет к оживлению процессов обновления версий ERP-систем в корпоративном секторе.

4) Таким образом, главным условием успешного развития такого актуального направления современных информационных технологий, как создание систем интеллектуальной поддержки принятия решения для предприятий сферы сервиса является четкая методологическая постановка решения задачи в заданной предметной области. Это условие, в первую очередь, предполагает выбор иерархии показателей, необходимых для оценки эффективности принятого решения и разработку методик для их определения.

Архитектура программных средств данного класса должна обеспечивать наиболее полную реализацию функциональных возможностей этих методик, их согласование по входным и выходным

данным между собой и сопряжения с общей базой данных, централизованное и децентрализованное использование методик, возможность модернизации и наращивания программных средств, а также - интегрирования усилий разработчиков (организаций) при создании сложных систем. При этом реализация таких противоречивых требований к их архитектуре находится в достаточно сильной зависимости от степени научного развития принципов их разработки и обоснованного выбора соответствующей технологии.

И в этом смысле, представляется перспективным организация и проведения соответствующих научно-исследовательских работ, а также открытие в рамках направления «Прикладная информатика в сфере сервиса» магистерской программы «Системы интеллектуальной поддержки принятия решений».

СПИСОК ЛИТЕРАТУРЫ

1. Кудряшев Н.В., Лобов С.А., Пуха Г.П. Методология разработки и применения в учебном процессе систем интеллектуальной поддержки принятия решения // Тезисы докладов межрегиональной конференции СПбГУ телекоммуникаций. СПб, СПбГУ, 1997. с. 112–120
2. Материал из Википедии — свободной энциклопедии
3. Turban, E. Decision support and expert systems: management support systems. -Englewood Cliffs, N.J.: Prentice Hall, 1995. — 887 p.
4. Карцев С.А. Совершенствование управления предприятиями на основе современных web-технологий и систем документооборота //Теория и практика сервиса: экономика, социальная сфера, технологии №2(8)/2011. СПб.: СПбГУСЭ. 2011.
5. Пуха Г.П. Разработка информационных систем в интегрированных системах визуального программирования: учеб. пособие для студентов высш. учеб. заведений. СПб.: Изд-во ИИГ «АКТиБ», 2008. 205 с. (Высшая школа).
6. Пуха Г.П. Анализ и синтез системы тактической связи группировок разнородных сил (учебно-методическое пособие для выполнения курсовых и дипломных работ). СПб., ВМА, 1995, 117 с.
7. Кадеев Д.Н. Информационные технологии и электронные коммуникации. Курс лекций. http://emf.ulstu.ru/metod/ITEK/index.htm.
8. http://ru.wikipedia.org/wiki/ERP#cite_note-.D0.9B.D0.B5.D0.BE.D0.BD
9. .E2.80.942008.E2.80.94.E2.80.9414-1.
10. Любарский Ю.Я. Интеллектуальные информационные системы. М.: Наука, 1990. 228 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗДРАВООХРАНЕНИИ

УДК 57.087

ЗАКОНОМЕРНОСТЬ РАСПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ ТРЕВОЖНОСТИ ВЗРОСЛОГО ЧЕЛОВЕКА

Бланк Михаил Аркадьевич[1], Бланк Ольга Алексеевна[1], Мясникова Екатерина Марковна[2], Рудницкий Сергей Борисович[3], Денисова Дарья Михайловна[3]
[1]Федеральное государственное бюджетное учреждение «Российский научный центр радиологии и хирургических технологий» Министерства здравоохранения Российской Федерации
Россия, Санкт-Петербург, п. Песочный, Ленинградская ул., д. 70
[2] Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, Политехническая ул., д. 29,
[3]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия В.О., д. 39
e-mails: mablank@mail.ru, oablank@mail.ru, ekmyasnikova@yandex.ru, sbr@spiiras.ru, dendm@spiiras.ru

Аннотация: В статье рассматриваются выявленные в ходе исследования особенности распределения показателей ситуативной тревожности у онкологических больных, проходящих курс противоопухолевой терапии.

Ключевые слова: *ситуативная тревожность; личностная тревожность; распределение показателей; злокачественные новообразования.*

Distribution patterns of anxiety rates in adult humans

Blank Mikhail Arkadievich[1], Blank Olga Alexeevna[1], Myasnikova Ekaterina Markovna[2], Rudnitsky Sergey Borisovich[3], Denisova Daria Mikhailovna[3]
[1]Federal government-financed research establishment, Russian Research Centre for Radiology and Surgical Technologies (RRCRST)
Russia, Saint Petersburg, Pesochny, Leningradskaya st, 70
[2]Saint-Petersburg State Polytechnical University (SPbPU),
Russia, Saint Petersburg, Politekhnicheskaya st., 29,
St. Petersburg, Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line, 39,
e-mails: mablank@mail.ru, oablank@mail.ru, ekmyasnikova@yandex.ru, sbr@spiiras.ru, dendm@spiiras.ru

***Abstract*:** Research reveals distribution patterns of state anxiety rate in cancer patients undergoing antitumor treatment.

Keywords: *state anxiety, trait anxiety; rate distribution; cancer.*

Введение. Критериями, определяющими эффективность лечения онкологических больных, служат не только непосредственные и отдалённые результаты проведённого воздействия (хирургического вмешательства, лекарственной противоопухолевой терапии, лучевой терапии), но и качество жизни пациента.

Непосредственные результаты лечения определяют, оценивая степень регресса опухоли, и констатируют полный либо частичный регресс злокачественного новообразования, стабилизацию или прогрессирование процесса. В качестве отдалённых результатов противоопухолевого воздействия принято учитывать среднюю продолжительность жизни пациентов и выживаемость в течение определённого срока (процент больных, проживших от момента установления диагноза, например, 1, 3, 5 или 10 лет).

В последние десятилетия мероприятия по сохранению удовлетворительного качества жизни пациента в период проведения и по завершении курса лечения злокачественного новообразования встало в один ряд с приоритетными прежде разработками, направленными на улучшение непосредственных и отдалённых результатов противоопухолевых воздействий.

Качество жизни индивидуума зависит не только от наличия и выраженности соматических страданий (болевого синдрома, нарушения функций органов и систем), от степени нарушения физической и умственной активности, обеспечивающих сохранение или утрату трудоспособности и возможности самообслуживания, от социальной поддержки и адаптации, но и от психологического статуса человека.

Известно, что психологическое состояние пациента не только в значительной мере определяет качество его жизни, но и влияет на эффективность проводимого лечения [4], [5], [6]. В перечне известных ныне факторов, от которых может зависеть результат специфических противоопухолевых воздействий [2], отведено немаловажное место именно психологическим факторам. Правильное представление об особенностях психологического статуса больного на разных этапах течения опухолевого процесса (в момент установления первичного диагноза, во время проведения всего курса лечения, в период ремиссии, в случаях рецидива заболевания, в терминальной стадии) необходимо и для рациональной организации психологического сопровождения пациентов, а также для оптимального построения отношений «больной – врач» и «врач – больной». Современный тренд развития медицины – «персонификация» лечебного воздействия – предусматривает формирование и реализацию плана лечения с учётом не только особенностей соматического статуса конкретного пациента и подробных характеристик (вплоть до генетических) заболевания, но и с коррекцией, соответствующей психотипу каждого пациента и его психологическим реакциям на заболевание.

Одним из основных показателей, отражающих психологические особенности человека, является присущая данному индивидууму личностная тревожность. На изменения обстоятельств (в данном случае – состояние болезни, получение информации о наличии значимой угрозы жизни) человек реагирует изменением уровня ситуативной тревоги. Существует устоявшееся мнение о повышении уровня ситуативной тревоги у всех онкологических больных.

Статистические исследования в области психологии и математическая обработка полученных данных сопряжены с определёнными трудностями. Количественную оценку психологических особенностей личности и реакций на изменение ситуации производят с использованием так называемых «мягких» шкал. Тем более важным становится корректный выбор методов статистики для получения результатов, адекватно характеризующих изучаемые нематериальные параметры и позволяющих делать правильные выводы и заключения.

1. Материалы и методы. Ранее, при выполнении плановой научной работы, посвящённой созданию инструмента для оценки психосоматического состояния человека [3], [8], нами была создана обширная база данных, позволившая выполнить настоящее исследование, целью которого явилось изучение возможных особенностей психологического статуса онкологических больных, находящихся в процессе лечения. Для этого решались следующие задачи:

1) определение показателей тревожности практически здоровых лиц;

2) изучение тревожности беременных женщин (положительный контроль);

3) установление показателей тревожности больных злокачественными новообразованиями, получающих специфическую противоопухолевую терапию;

4) определение показателей тревожности онкологических больных, введённых в длительную (≥4-5 лет) клиническую ремиссию.

Материалом для исследования послужили данные компьютерного опроса состояния тревожности в группах, соответствующих поставленным задачам, а именно:

1) практически здоровых взрослых людей, прошедших полноценное обследование во время диспансеризации (99 человек, 103 исследования);

2) беременных женщин (171 женщина, 196 исследований);

3) больных злокачественными новообразованиями различных локализаций (23 человека, 39 исследований), находящихся в процессе специфического лечения;

4) больных злокачественными новообразованиями (42 человека, 79 исследований), введённых в длительную клиническую ремиссию.

Все исследуемые подвергались тестированию, для чего был использован Интегративный тест тревожности (ITT) компьютерный вариант для взрослых, разработанный в Психоневрологическом институте им. В.М. Бехтерева [1], [7] и отражающий такие составляющие, как неспецифический эмоциональный дискомфорт, астенический компонент, фобический компонент, тревожную оценку перспективы и компонент социальной защиты. Выбор Интегративного теста тревожности обусловлен тем, что ITT позволяет количественно оценить перечисленные проявления личностной тревожности и ситуативной тревоги. Тест понятен и прост, анкеты опросника доступны для самостоятельного заполнения испытуемыми, обладающими минимальной компьютерной грамотностью. Обработка данных производится автоматически. Всё обследование занимает не более 10-15 минут и может быть реализовано на амбулаторном врачебном приёме в любом медицинском учреждении.

В соответствии с дизайном планового исследования были сформированы две исследовательские и две контрольные группы. В первую исследовательскую группу вошли больные с морфологически верифицированным диагнозом злокачественного новообразования

(злокачественные лимфомы и солидные опухоли), проходившие тестирование в период проведения специфического противоопухолевого лечения. Вторую исследовательскую группу составили пациенты, введённые в длительную (не менее трех лет) клиническую ремиссию и находящиеся под динамическим наблюдением в ФГБУ РНЦ РХТ. Эти лица не реже одного раза в год подвергались полному физикальному, клинико-лабораторному и лучевому обследованию, подтверждавшему ремиссию заболевания. Подавляющая часть группы представлена больными злокачественными лимфомами. Группа положительного контроля сформирована из практически здоровых волонтёров, прошедших углубленную диспансеризацию и получивших допуск к работе с источниками ионизирующего излучения. В группу отрицательного контроля были включены практически здоровые беременные женщины, обследованные и находящиеся под наблюдением в одной из женских консультаций Санкт-Петербурга. Расчёты статистических критериев произведены с помощью пакета Statistica 6.0 и функции dip.test пакета R.3.00.

2. Особенности распределения показателей тревожности в группах. В результате сравнительного анализа характера распределения интегративных показателей тревожности в исследованных группах выявлено следующее: в группе здоровых лиц, как и в группе беременных, ни ситуативная тревога, ни личностная тревожность не соответствуют закону «нормального» распределения (рисунок1, гистограммы 1a, 1b и 2a, 2b). Оба эти показателя тревожности в указанных группах проявляют тенденцию к бимодальному распределению.

Аналогичная картина наблюдается и в группе больных злокачественными новообразованиями, введённых в длительную клиническую ремиссию (рисунок1, гистограммы 4a, 4b), в которой так же, как и в двух вышеупомянутых группах, оба показателя интегративной тревожности проявляют тенденцию к бимодальности.

Совсем иная картина наблюдается в группе больных, находящихся в процессе специфического противоопухолевого лечения по поводу злокачественных новообразований. Если в отношении показателей личностной тревожности, как и во всех предыдущих группах, наблюдается проявление тенденции к бимодальности (рисунок 1, гистограмма 3b), то в отношении характера распределения показателей ситуативной тревожности очевидна ярко выраженная тенденция к формированию унимодального распределения (рисунок1, гистограмма 3a).

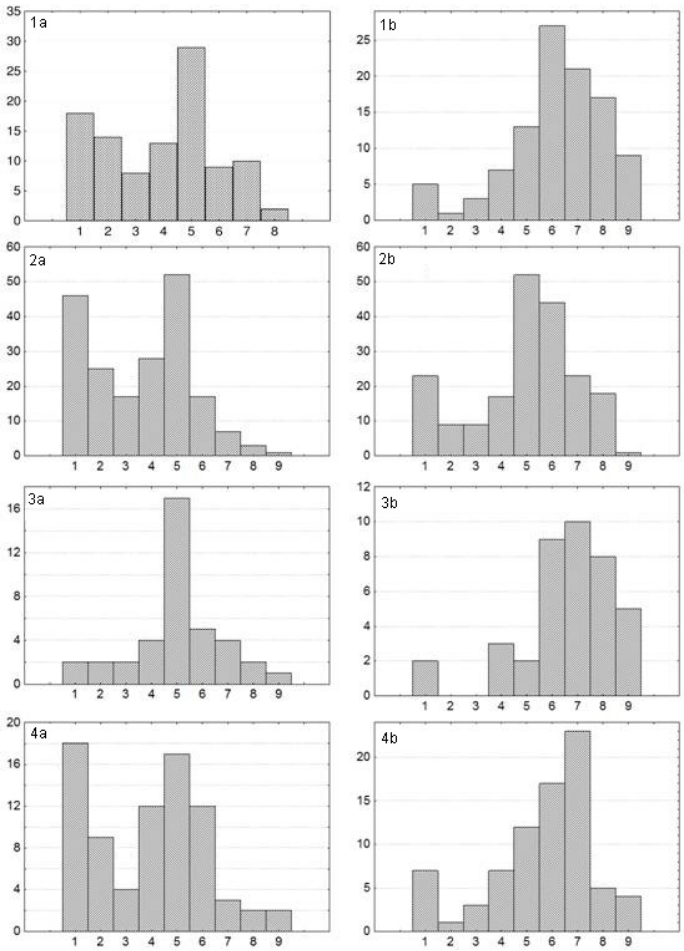


Рис.1. Гистограммы распределения интегративных показателей ситуативной (a) и личностной (b) тревожности у здоровых взрослых людей – 1, беременных женщин – 2, онкологических больных, проходящих лечение – 3 и онкологических больных, введённых в устойчивую клиническую ремиссию – 4.

Выводы, сделанные на основании визуального анализа гистограмм показателей тревожности, подтверждаются с помощью статистических методов. Так, попарное сравнение четырёх групп по критерию Колмогорова-Смирнова показывает значимое ($p<0.05$) отличие показателей ситуативной тревожности третьей группы от остальных групп. При этом все остальные группы значимо не различаются между собой ($p>0.1$ для всех попарных сравнений). Дополнительно был проведен DIP-тест на унимодальность распределения [9], который показал, что гипотеза унимодальности отвергается с уровнем значимости $p< 10\text{-}7$ для всех групп кроме третьей. Значение p-уровня для третьей группы составляет 0.28, что значимо свидетельствует об унимодальном распределении показателей.

Заключение. Во всех исследованных группах распределение показателей, как ситуативной тревоги, так и личностной тревожности, проявляя бимодальность, не соответствует закону нормального (Гауссова) распределения, что свидетельствует о некорректности использования методов, требующих нормальности распределения вектора данных. Как следствие, применение неадекватных статистических подходов может приводить к формированию ошибочных представлений.

Нами установлено, что только в отношении показателей ситуативной тревожности онкологических больных, получающих лечение, распределение этих показателей носит ярко выраженный унимодальный характер, который исчезает в группе больных, введённых в длительную ремиссию. Выявленный нами феномен является неожиданным, поскольку противоречит сложившемуся представлению о повышении тревожности у онкологических пациентов.

Можно предположить, что обнаруженное в результате нашего исследования бимодальное распределение показателей личностной тревожности и ситуативной тревоги у людей, пребывающих в различных жизненных ситуациях, таких как здоровье и активная трудовая деятельность, ожидание ребёнка, восстановление активности и адаптации после успешного проведения курса противоопухолевого лечения при наличии диагноза онкологического заболевания, отражает распределение общеизвестных психотипов человека в популяции.

Феномен изменения показателей ситуативной тревоги в группе онкологических больных, пребывающих в процессе лечения, мы объясняем изменением реакции на реальную и значимую угрозу жизни вследствие разделения или перемещения ответственности за исход на других лиц (лечащего врача, другой медицинский персонал).

Изучение причин этого явления лежит в сфере интересов и профессиональной деятельности клинических психологов.

Можно предположить, что установленная нами закономерность «усреднения» показателей ситуативной тревоги распространяется не только на больных злокачественными новообразованиями, получающих квалифицированное лечение, но и на пациентов, страдающих от неонкологических заболеваний, угрожающих их жизни, и имеющих возможность разделить ответственность за исход с медицинским персоналом.

СПИСОК ЛИТЕРАТУРЫ

1. Бизюк А.П., Вассерман Л.И., Иовлев Б.В. Применение интегративного теста тревожности (ИТТ). Методические рекомендации. СПб.: Изд-во НИПНИ им. В. М. Бехтерева, 2003, 23 с.
2. Бланк М.А., Бланк О.А. Хронобиомедицина для онкологии. СПб., NIKA. 2010. 120 с
3. Бланк М.А., Рудницкий С.Б., Бланк О.А., Вассерман Е.Л., Вильнер Г.А., Жвалевский О.А., Денисова Д.М., Ширяева О.А. К оценке психосоматического статуса человека. Материалы научной конференции «От лучей Рентгена – к инновациям XXI века: 90 лет со дня основания первого в мире рентгенорадиологического института (Российского научного центра радиологии и хирургических технологий)» (с участием специалистов стран ближнего и дальнего зарубежья) 8-10 октября 2008 г. Санкт-Петербург, с. 343.
4. Гнездилов А.В. Путь на Голгофу. СПб. Фирма «КЛИНТ», 1995, 136 с.
5. Колосов А.Е., Шиповников Н.Б. Психологические нарушения при диагнозе «рак». Киров, «Вятка», 1994, 136 с.
6. Мишин Ю.Б. Философия рака. Этиология, патогенез, лечение и профилактика: Заметка практикующего врача-онколога. Волгоград. Волгоградское научное издательство. 2005, 108 с.
7. Червинская К.Р., Щелкова О.Ю. Медицинская психодиагностика и инженерия знаний / Под ред. Л.И.Вассермана. СПб.: Ювента; М.: Издательский центр «Академия», 2002, 624 с.
8. Юсупов Р.М., Вассерман Е.Л., Денисова Д.М., Дюк В.А., Жвалевский О.В., Карташев Н.К., Рудницкий С.Б., Толстоногов Д.А., Бланк М.А., Бланк О.А. Разработка теоретических основ, моделей и информационных технологий экспресс-диагностики и мониторинга функционального состояния человека на основе комплексной обработки биометрических данных. РАН Программа фундаментальных исследований Президиума РАН. Фундаментальные науки – медицине. (Конференции и семинары по научным направлениям Программы в 2009 году). М.: Фирма «Слово», 2009. с.105-106.
9. Hartigan J.A., Hartigan P.M. The DIP test of unimodality. The Annals of Statistics. 1985, V.13, pp. 70-84.

УДК 502.084

СОБЫТИЙНАЯ МОДЕЛЬ БАЗЫ ДАННЫХ ИНТЕГРИРОВАННЫХ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ ДЛЯ РЕШЕНИЯ ЗАДАЧ МЕДИЦИНСКОЙ СТАТИСТИКИ

Блюм Владислав Станиславович,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия В.О., 39,
e-mails: vlad@blum.spb.su

Аннотация: Государственная система сбора и обработки медицинских статистических данных ежегодно выполняет сбор и обработку более пятидесяти тысяч параметров. Результаты этой работы необходимы для обоснованного выбора направлений развития системы здравоохранения. В работу государственной системы медицинской статистики вовлечены значительные людские ресурсы, деятельность которых часто вступает в противоречие с лечебно-диагностическим процессом, отвлекая медицинский персонал. При этом оперативность получения статистических данных и их достоверность вызывают серьёзные нарекания. Решить указанные проблемы и значительно сократить затраты на содержание системы государственной медицинской статистики призвана инновационная технология сбора и обработки потока первичной медицинской информации, основанная на формировании региональных и федеральной баз интегрированных электронных медицинских карт. Рассмотрена и обоснована модель динамического, полного пространства событий в клинической сфере здравоохранения. Приведён состав основных алгоритмов над базой интегрированных медицинских карт, решающих проблему оперативного и достоверного сбора актуальных статистических данных для обоснованного принятия решений при управлении системой здравоохранения.

Ключевые слова: *Информатизация здравоохранения; медицинская статистика; интегрированная электронная медицинская карта.*

EVENT MODEL DATABASE OF INTEGRATED EHR FOR SOLVING THE PROBLEMS OF MEDICAL STATISTICS

Blum Vlad,
St. Petersburg, Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line V.O., 39,
e-mails: vlad@blum.spb.su

Abstract: State system for the collection and processing of medical statistics annually performs the collection and processing of more than fifty thousand parameters. The results of this work are needed to make informed choices trends in the development of the health system. In the state system of health statistics are thousands of people who often distract health workers from the diagnostic and treatment process. In this case, the efficiency of obtaining statistical data and the accuracy of the cause serious complaints. To solve these problems and greatly reduce the cost of maintaining the system of public health statistics innovative technology is designed to collect and process flow of the primary health information, based on the formation of regional and federal databases integrated electronic medical records. Reviewed and substantiated the dynamic model, the total space of events in clinical health care. Is given the composition of the basic algorithms over the base of integrated medical records, solving the problem of timely and reliable collection of relevant statistical data for informed decision-making in the management of the health system.

Keywords: *Health information; medical statistics; integrated electronic medical record.*

Введение. Нет оснований подвергать сомнению значение медицинской статистики для управления системой здравоохранения. Однако, со всё большей остротой ощущаются её (медицинской статистики) недостатки, как то:

– отрыв медицинского персонала, задействованного в лечебно-диагностическом процессе, на обеспечение сбора статистических данных;

– недостаточная (по современным меркам) оперативность формирования статистических данных, не позволяющая эффективно маневрировать ограниченными ресурсами здравоохранения;

– обоснованные претензии к достоверности собранных статистических данных, которые возникают из-за непреодолимого человеческого фактора.

Следует указать на наметившийся процесс трансформации статистики из инструмента оценки и осознания российской реальности в пропагандиста успехов руководителей страны. Изменить эту тенденцию вряд ли удастся переходом от методик оценки Глобального Бремени Болезней (ГББ) к методикам оценки Глобальных Сравнительных Описательных Эпидемиологий (ГСОЭ). Причина

кроется прежде всего в том, что роль пропагандиста выполняет финансируемая государством, дорогостоящая система сбора и обработки медицинской статистики: 2254 врача-статистика, 10696 медицинских статистиков, 16 Бюро медицинской статистики, отделы медицинской статистики в составе 83-х медицинских информационно-аналитических центров [14]. При этом, обеспеченность компьютерным оборудованием этой армии статработников составляет 5,5 единиц на 1 кабинет, то есть существенно лучше, чем у лечащих врачей. По самым скромным подсчётам, содержание этой системы «лукавых» цифр, производящей более 60 тыс. показателей в год (см. пост http://www.gosbook.ru/node/87357), обходится государству более 3 млрд. рублей в год, без учёта финансовых потерь, связанных с отрывом лечащих врачей на участие в сборе статистической информации о своей работе.

Необходимость верификации статистических данных очевидна. Существует мнение, что эта цель может быть достигнута за счёт повышения информативности интегральных показателей, то есть, за счёт использования не одного медико-демографического показателя, а совокупности обобщенных индексов, которые должны позволить описывать ситуацию по регионам, причинам заболеваний и травмам, возрастно-половым группам с помощью согласованной системы индексов таких, как смертность (mortality), годы потерянной жизни (YLL), годы жизни, прожитые с нарушениями здоровья (YLD), потерянные годы здоровой жизни (DALY), а также трёх аспектов по заболеваниям и факторам риска: абсолютное число потерь, коэффициент потерь, доля потерь от отдельных заболеваний по отношению к общим потерям [14]. Но при этом очевидно, что начинать следует с достижения полноты и достоверности исходной (первичной) медицинской информации.

В связи с интенсивным развитием телекоммуникационной инфраструктуры здравоохранения и реализацией проекта единой государственной системы (ЕГИС) можно предложить инновационный путь решения указанных проблем.

В своё время, профессор В.М. Тавровский [13], [14] высказал тезис о том, что база электронных историй болезни является необходимым и достаточным основанием для извлечения всех без исключения статистических параметров о лечебно-диагностическом процессе. Пришло время внедрить в практику это утверждение.

Постановка задачи: над федеральной базой интегрированных электронных карт (ИЭМК) разработать программный комплекс сбора и обработки медицинских статистических данных (ПК СОМС), способный заменить в полной мере существующую государственную систему медицинской статистики.

С экономической точки зрения решение указанной задачи оправданно, поскольку разработка и эксплуатация такого программного комплекса вряд ли будет стоить государству более 3 млрд. рублей в год. При этом очевидны этапы внедрения новой технологии.

О непроизводительном отрыве медицинских работников для обслуживания указанного программного комплекса речи быть не может, поскольку врачи и диагностические лаборатории в предлагаемой технологической схеме выполняют только традиционную работу, формируя электронные персональные медицинские записи (ЭПМЗ), а доставка ЭПМЗ в базу электронных медицинских карт ЛПУ и далее в федеральную базу ИЭМК выполняется без их участия.

В результате работы программного комплекса, размещенного в федеральном центре обработки данных (ЦОД), мы вправе ожидать получения достоверных статистических данных не через месяц, полгода, год, а в режиме реального времени с любой детализацией по регионам, возрастам и социальным группам.

Некоторые определения и способы идентификации

Персональная медицинская запись – это элемент бинарного отношения, который документально фиксирует конкретную встречу квалифицированного источника медицинской информации с пациентом.

Квалифицированными источниками медицинской информации (КИМИ) были и остаются врачи (и их доверенные лица) и медицинские диагностические лаборатории. Квалификация КИМИ и их право доступа к телу пациента подтверждается дипломами, аттестациями, сертификатами и лицензиями.

Формальное определение электронной персональной медицинской записи (ЭПМЗ) должно базироваться, в первую очередь, на строгом учёте и использовании исключительно КИМИ в качестве авторов ЭПМЗ. Верификация ЭПМЗ в любой медицинской информационной системе должна начинаться именно с проверки легитимности источника медицинской информации. Такой посыл позволяет довольно строго (на верхнем уровне) определить грамматику языка, называемого Интегрированной Электронной Медицинской Картой.

<ИЭМК>::=<упорядоченный по времени список ЭПМЗ> (1)

<ЭПМЗ>::=<дата и время сеанса><ID КИМИ><ID пациента><документ КИМИ> (2)

Не раскрывая далее (за недостатком места) приведённые грамматические категории заметим, что первой записью в ИЭМК должна быть запись врача о рождении нового пациента, а

заключительной – запись о смерти его мозга и, возможно, результаты патологоанатомического исследования. Полнота ИЭМК, то есть присутствие в ней всех без исключения событий, связанных со встречами пациента с КИМИ, есть то необходимое условие, при выполнении которого появление программ раннего обнаружения дефектов оказания медицинской помощи станет объективной реальностью.

В первую очередь, следует договориться о способе идентификации пациентов и КИМИ.

На наш взгляд, конструктивным способом формирования идентификатора пациента и его интегральной электронной медицинской карты может стать код, составленный из даты рождения пациента и учётного номера на данную дату в федеральной базе ИЭМК. Этот учётный номер не может быть в России более 5-значного десятичного числа при средней рождаемости 5 тысяч человек в день.

<ID ИЭМК>::=<ID пациента>::=<дата рождения><порядковый учётный номер>

Ведение государственного реестру КИМИ и доступ к нему также становится одной из первоочередных задач. При этом идентификатор врача может базироваться на <ID пациента>, поскольку каждый врач одновременно является пациентом, то есть

<ID врача>::=<ID пациента><список учётных номер специалиста>

Идентификатор диагностической лаборатории может опираться на дату получения соответствующей лицензии. Например,

<ID диагностической лаборатории>::=<дата лицензирования><учётный номер>

Заметим, что врач может иметь довольно длинный <список учётных номер специалиста>, поскольку в течение профессиональной практики получает дополнительные квалификации и может выполнять свои функции не в одном, а в нескольких лечебно-профилактических учреждениях и работать в качестве индивидуального предпринимателя.

Предлагаемый способ идентификации ИЭМК отличается тем, что персональная карта пациента получает уникальный идентификатор, который обеспечивает оперативные и гарантированный доступ к базе федеральной «регистратуры» с момента рождения пациента до его смерти. Этот код создаётся при самой первой попытке разместить ЭПМЗ в ИЭМК пациента и после этого идентификатор не будет меняться на протяжении всего срока хранения данной ИЭМК. Важным свойством такого способа идентификации является то, что он задаёт отношение строгого порядка на множестве всех ИЭМК. Более того, появление нового, ранее не известного, пациента любого возраста в поле зрения системы здравоохранения не нарушает отношение строгого порядка в базе ИЭМК, а значит, не потребует её перестройки в будущем. И, наконец, база ЭМК в каждом ЛПУ может рассматриваться как извлечение из федеральной базы ИЭМК при сохранении системы идентификаторов и отношения строгого порядка. Последнее обстоятельство следует использовать в качестве способа контроля достоверности любой ЭПМЗ.

Векторно-событийная модель федеральной базы ИЭМК

Опираясь на введённые определения и предложенный способ идентификации ИЭМК, может быть построена формальная модель базы федеральной базы ИЭМК. Целью данной модели является стремление предложить единую точку зрения на этот сложный информационный объект.

Согласно определению любая ЭПМЗ есть элемент списка ИЭМК, упорядоченного по времени создания ЭПМЗ. И, в этом смысле, ЭПМЗ фиксирует некоторое персонифицированное событие в системе здравоохранения.

Очевидно, что ЭПМЗ характеризуется определённым количеством информации, которая выражается в количестве бит электронной записи.

Векторный характер каждого события – ЭПМЗ, будем связывать с целенаправленным процессом оказания медицинской помощи и неравномерностью интегрального лечебно-диагностического процесса, который отражается в ИЭМК.

Для построения событийной модели базы ИЭМК [11] определим ортогональную систему координат, в которой осью абсцисс станет t_ρ – дискретная ось времени жизни популяции, а осью ординат будет непрерывная временная ось, которую назовём осью времени жизни пациентов и обозначим – t_τ . Начало координат определим, как самый ранний момент времени рождения пациента, история болезни которого, по каким-то причинам, сохранилась в архивах системы здравоохранения (рисунок 1), но так, чтобы все наши дальнейшие построения выполнялись в первом квадранте построенной системы координат.

Для самого возрастного пациента, идентификатор ИЭМК которого – I_{0s}, построим вектор $\vec{v}_{0s}$, длина которого $|\vec{v}_{0s}|$ будет равна реальному времени жизни этого пациента. Вектор $\vec{v}_{0s}$ разместим

параллельно оси t_τ с началом в точке I_{0s}, соответствующей дате рождения этого пациента. Очевидно, что $|\vec{v}_{0s}| = \Delta$ – время жизни пациента равное времени жизни популяции.

Покажем, что вектор $\vec{v}_{0s}$ есть проекция информационного вектора истории болезни на временную ось t_τ.

Построим соответствующие вектора $\vec{v}_{0i}$ для всех учтённых ИЭМК (имеющих идентификаторы – I_{0i}), но не имеющих ЭПМЗ – $z_f(i)$ о факте смерти пациента. Начало этих векторов будет лежать на оси t_ρ – в соответствии с датой рождения и учётным номером в рамках этой даты, а конец окажется одной из точек гипотенузы равнобедренного прямоугольного треугольника с катетом $|\vec{v}_{0s}|$.

Каждый из построенных векторов суть временной образ (проекция) истории болезни конкретного пациента, который, в свою очередь, состоит из суммы векторов, число которых соответствует числу ЭПМЗ в данной ИЭМК.

$\vec{v}_{0i} = \sum_{j=1}^{k} \vec{v}_j$, где k – число записей в ИЭМК i - го пациента, а $|\vec{v}_j|$ – интервал времени от данной ЭПМЗ до следующей, либо до текущего момента t_0. Заметим, что текущий момент времени рассматриваемом в пространстве $T \times T$ характеризуется прямой $y = -t + t_0$.

Прямоугольный треугольник, катетами которого являются вектор $\vec{v}_{0s}$ и отрезок оси t_ρ – $[I_{0s}, t_0]$, ограничивает временное пространство $\Omega \subset T \times T$, в котором размещены все, без исключения, актуальные события, которые фиксируют моменты возникновения ЭПМЗ вида (1) в системе здравоохранения (системе ныне здравствующих пациентов). Актуальными будем называть такие события, которые соответствуют ЭПМЗ здравствующих пациентов, то есть пациентов, в ИЭМК которых не содержится записи – $z_f(i)$.

Таким образом, мы построили ограниченное временное пространство Ω, в котором размещены и строго упорядочены ЭПМЗ всех ныне здравствующих потенциальных пациентов (рисунок 1).

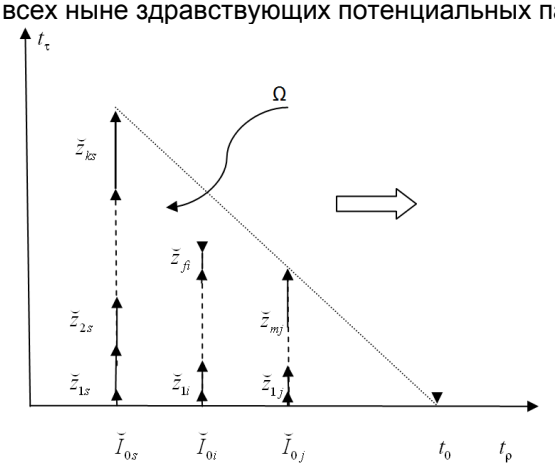


Рис. 1. Модель событий базы ИЭМК

В данной модели для текущего момента t_0 векторные образы ИЭМК всех учтённых живых пациентов упорядочены по величине (времени жизни пациента), а вершины их векторов лежат на одной прямой, которая является гипотенузой прямоугольного треугольника, ограничивающего временное пространство Ω. В пространстве $\Omega \subset T \times T$ размещены и строго упорядочены по оси t_ρ все ИЭМК, а по оси t_τ строго упорядочены все ЭПМЗ в векторах каждого пациента.

Гипотенуза равностороннего треугольника (пространства Ω) – это отрезок прямой $y = -t + t_0$, длиной $\sqrt{2}|\vec{v}_{0s}|$. Особенностью этого отрезка является то, что он определяет интерфейс системы здравоохранения. Именно на этом ограниченном отрезке, и только на нём, могут возникнуть новые события (ЭПМЗ) в данной модели системы охраны здоровья в текущий момент времени.

Интегрированная электронная медицинская карта – это сумма векторов ЭПМЗ, которая пополняется системой охраны здоровья на протяжении всей жизни пациента. Начиная с момента

рождения, система здравоохранения производит персональные медицинские записи (теперь – ЭПМЗ) и последовательно размещает их в истории болезни (теперь – ИЭМК). Каждая запись имеет собственное информационное наполнение. Не пытаясь на этом этапе оценивать семантику записи, мы всегда можем посчитать количество бит, необходимых для хранения данной ЭПМЗ в памяти компьютера. Ясно, что каждый бит такой записи, в той или иной степени несёт в себе информацию о ресурсах затраченных системой здравоохранения на данного пациента. Очевидно, что каждый вектор (ЭПМЗ) имеет фиксированную по величине (количеству бит) проекцию на информационно-временную плоскость $I \times T_\rho$ (см. рисунок 2).

Особенность предлагаемой информационной модели базы ИЭМК заключается в том, что, при сохранении неизменной величины проекций всех зафиксированных векторов ЭПМЗ на плоскость $I \times T_\rho$ (в записи не добавляется битов), проекция последней ЭПМЗ в каждой ИЭМК на плоскость $I \times T_\tau$ будет непрерывно увеличивается до момента появления очередной ЭПМЗ, что характеризует процесс старения информации.

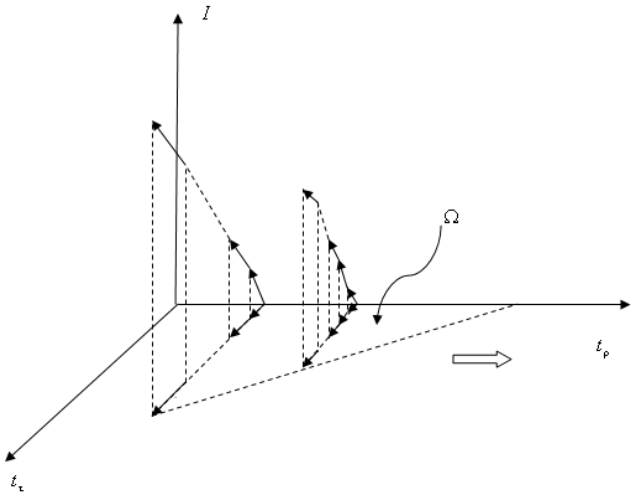


Рис. 2. Информационная модель базы ИЭМК

Вектор последней записи (ЭПМЗ) будет изменять величину и угол наклона к плоскости $I \times T_\tau$ вплоть до появления очередной записи. Каждая ИЭМК размещена в персональной для данного пациента информационно-временной плоскости ($I \times T$), которая характеризуется моментом рождения – $\breve{I}_{0i}$ (рисунок 3).

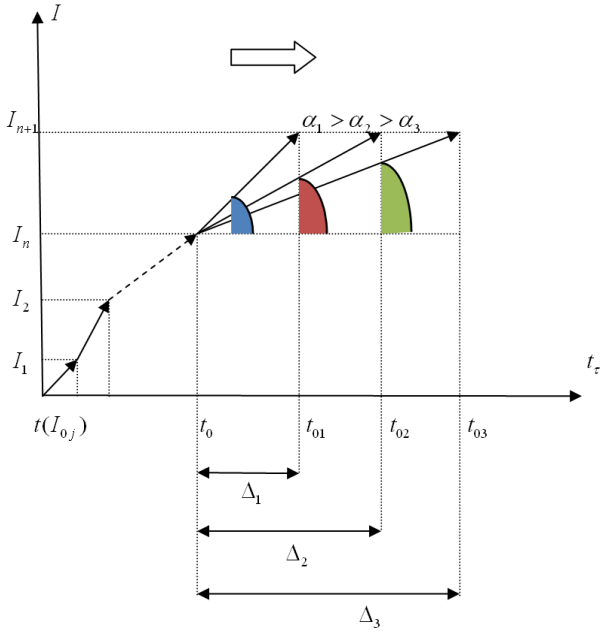


Рис. 3. Информационный вектор истории болезни

В результате анализа информационного вектора ИЭМК, может быть оценено не только его информационное наполнение (объём ресурсов здравоохранения, затраченных на пациента), но и, так называемый, «угол внимания» системы здравоохранения по отношению конкретному пациенту. Этот параметр важен при организации государственной системы диспансерного контроля состояния здоровья.

Рассмотрение персональной информационно-временной плоскости ИЭМК показывает, что при увеличении интервала времени между возникновениями двух последовательных ЭПМЗ $\Delta_1 < \Delta_2 < \Delta_3$ уменьшается угол наклона информационного вектора $\alpha_3 < \alpha_2 < \alpha_1$, что может быть использовано в качестве объективного критерия для учёта «оторвавшихся» от диспансерного наблюдения и организации профилактического контроля здоровья с учётом всей предыстории врачебных вмешательств.

Информационная составляющая ЭПМЗ является объектом семантического анализа и предполагает наличие нового класса программных агентов для оперативной оценки эффективности использования ресурсов здравоохранения и раннего обнаружения дефектов оказания медицинской помощи в результате обработки полной, достоверной и доступной для автоматизированной обработки информации в базе ИЭМК.

Заметим, что, при использовании предложенного подхода, извлечение из федеральной базы ИЭМК данных о «своих» пациентах для конкретного ЛПУ или региона не приведёт нарушению отношения строгого порядка в соответствующей локальной базе данных.

В качестве первого шага отработки функционала федеральной базы ИЭМК могло бы стать решение более простой, чем обработка семантики ЭПМЗ, технологической задачи.

Таким, экономически оправданным, шагом к постоянному использованию федеральной базы ИЭМК может стать реализация проекта программного комплекса сбора и обработки статистической медицинской информации. Целью этой разработки должно стать стремление заменить существующую государственную систему медицинской статистики на такую, которая свободна от субъективных оценок и способна предоставить гораздо более полную и оперативную информацию для управления ограниченными ресурсами здравоохранения и, в то же время, высвободить значительные материальные и людские ресурсы.

Состав и функции государственной системы медицинской статистики

Российская система здравоохранения включает более восьми тысяч больниц всех типов, амбулаторно-поликлинических учреждений – 17,5 тысяч, диспансеров – 1,5 тысяч, стоматологических поликлиник и кабинетов – 26,5 тысяч, станций скорой медицинской помощи – более трех тысяч [http://www.gks.ru/]. Суммарно все эти подразделения оформляют более 430 тысяч отчетных и учетных форм. За последние пятьдесят лет число учетных форм увеличилось в три раза, а число отчетных форм – почти в четыре раза [4]. Основная нагрузка по сбору, контролю за заполнением, обработкой, хранением, а также анализом этой информации приходится на врачей статистиков и средних медицинских статистиков (2254 врача-статистика, 10696 медицинских статистиков). При этом число врачей статистиков на протяжении последних пяти лет практически не менялось, а число средних медицинских статистиков снижается. Государственная система медицинской статистики объединяет шеснадцать Бюро медицинской статистики, а также отделы медицинской статистики в составе 83-х медицинских информационно-аналитических центров. Подразделения медицинской статистики оснащены средствами вычислительной техники, в среднем 5,5 компьютеров на один кабинет, что существенно выше оснащения лечащих врачей компьютерной техникой [5].

Отметим, что все выше названные сотни тысяч учётных и отчётных форм являются производными данными от потока первичной медицинской информации, которую порождает лечебно-диагностический процесс и которая фиксируется в историях болезни пациентов, а в ближайшей перспективе – в базе ИЭМК. Это касается и фактов рождения и смерти, и выявленных диагнозов, также как, и фактически занятых лечебных коек.

Чтобы оценки медицинской статистики были доступны для объективного анализа и сопоставимы как на региональном, так на международном уровнях, они должны базироваться на Международной классификации болезней (МКБ). Это универсальный статистический инструментарий, который определил такую область нового познания, как статистика заболеваемости и смертности. МКБ предусматривает различные иерархические ступени ранжирования статистической информации – класс, блок, рубрика и подрубрика. В соответствии с этими ступенями и должны строиться программы сбора информации. Кроме того, Всемирной Организацией Здравоохранения (ВОЗ) предусмотрены и адаптированные классификации для специализированных служб здравоохранения, что позволяет более глубоко анализировать клиническую работу врачей без излишней формализации изучаемых явлений.

Российская медицинская статистика ежегодно формирует порядка 60 тысяч параметров [6]. Очевидна избыточность предлагаемых данных для эффективного управления здравоохранением.

При этом, всё более проявляется тенденция к целенаправленному искажению данных для демонстрации якобы «успехов».

Решая задачу кардинального изменения структуры государственной системы медицинской статистики, следует подвергнуть всесторонней ревизии состав и значимость системы статистических параметров, ранжировать требования к оперативности их использования в различных звеньях системы управления здравоохранением.

Есть основание утверждать, что, при исполнении ряда условий, практически все функции системы медицинской статистики сможет взять на себя программный комплекс сбора и обработки статистических данных, извлекаемых из федеральной базы ИЭМК.

Рассмотрим, какие условия должны быть выполнены для эффективной работы инновационной системы медицинской статистики и как их выполнение связано с современными направлениями информатизации здравоохранения.

Условия создания инновационной системы государственной статистики

Естественный процесс перехода от бумажного документооборота к электронному, в том числе, в клинической сфере здравоохранения, а также принятые решения по созданию телекоммуникационной инфраструктуры и мощных центров (региональных и федерального) обработки медицинских данных, позволяют ставить инновационные задачи информатизации здравоохранения. Одной из таких задач и является качественное изменение государственной системы медицинской статистики, которая в свою очередь может стать локомотивом для постановки и решения более сложных задач информационной поддержки лечебно-диагностических процессов в России.

Однако, кроме указанных трендов и научно-технических заделов, необходимо согласованное и директивное решение ряда технологических и организационных проблем.

В качестве первой проблемы такого рода должно стать законодательно утверждённое положение, согласно которого каждая вновь созданная электронная персональная медицинская запись при сохранении в базу данных конкретного лечебно-диагностического учреждения (ЛПУ) должна одновременно отправляться в централизованную базу ИЭМК.

Из этого требования вытекает необходимость внедрения единого для всей страны алгоритма и соответствующей технологии присвоения уникального идентификатора ИЭМК пациента. Данный идентификатор должен использоваться на протяжении всей жизни пациента и стать обязательным атрибутом каждой ЭПМЗ данного пациента. Предложенный выше способ идентификации может рассматриваться как один из рабочих вариантов решения данной проблемы. Достоинством такого подхода является то, что он предполагает очевидный диалоговый алгоритм взаимодействия источника медицинской информации (автора ЭПМЗ) с федеральным ЦОД, в том случае, когда данная ЭПМЗ является первой для данного пациента. Результатом этого диалога должно быть открытие в ЦОД новой ИЭМК. Для новорождённого пациента первой записью окажется реальная ЭПМЗ врача родильного дома. Для взрослого пациента кроме текущей ЭПМЗ в базу ИЭМК будет помещена формальная ЭПМЗ, фиксирующая момент его рождения и размещённая в очередной позиции на данную дату в «регистратуре» федеральной базы ИЭМК.

Ещё одним важным требованием является наличие в федеральном ЦОД актуальной базы данных, в которой хранится полный реестр квалифицированных источников медицинской информации (КИМИ). Реестр КИМИ может формироваться, как при получении источником соответствующего разрешения, так и оперативно, в режиме диалога с федеральным ЦОД при первой попытке разместить, изготовленную данным КИМИ, ЭПМЗ. В дальнейшем идентификатор КИМИ отмечает в базе ИЭМК все ЭПМЗ, которые были выполнены данным источником. Проще говоря, из базы ИЭМК может быть извлечена вся история врачевания данного КИМИ.

Наконец, важным требованием, но на первом этапе не самым критичным, должно стать формальное определение языка ЭПМЗ и разработка соответствующих ГОСТов. В частности, при раскрытии грамматической категории <ЭПМЗ> (см. формулу 2) должны быть уже на первом этапе строго определены терминальные символы, на основе которых из базы ИЭМК будут извлекаться необходимые статистические данные.

Инновационная государственная система медицинской статистики

Рассмотрим инновационную систему государственной медицинской статистики (ИГСМС), как многоагентный программный комплекс, реализованный на средствах сети (федерального и региональных) ЦОД.

Многоагентный подход широко используется в создании программных модулей интеллектуальных информационных систем – от выполнения задач поиска информации и распознавания образов до принятия решений, в том числе управленческих.

Основанием для применения такого подхода является большой объём информации, высокая динамика изменений и распределённый характер хранения информационного объекта, который представляет собой ИЭМК, с учётом её дублирующих компонентов.

Опираясь на предложенную в данной статье формальную векторно-событийную модель базы ИЭМК, определим основные требования к функциям и составу многоагентного программного комплекса (МАПК) сбора и обработки медицинской статистики (СОМС).

МАПК состоит из автономных агентов, способных воспринимать ситуацию, принимать решения и взаимодействовать с себе подобными. Знания, необходимые для такой системы, отделены от ее программного кода и хранятся в онтологии, представляющей собой сеть понятий и отношений предметной области.

Онтология МАПК СОМС, в частности, включает:

– формально определённую, актуальную структуру системы здравоохранения, реализующую интегральный лечебно-диагностический процесс (база ЛПУ, база станций скорой медицинской помощи и т.п.),

– актуальный реестр квалифицированных источников медицинской информации,

– и ряд других понятий и отношений.

Программный агент есть активная программа, выполняющая непрерывный мониторинг динамической системы данных, в данном случае базы ИЭМК, которая ежедневно пополняется более чем миллионом новых записей.

Функционирование агентов осуществляется в рамках агентной платформы – среды, в которой могут существовать и взаимодействовать агенты [1], [2]. В качестве агентной платформы для МАПК СОМС целесообразно рассматривать операционную среду федерального ЦОД.

МАПК обладает следующими свойствами:

– структура сообщества агентов является динамической относительно типов и количества членов сообщества;

– сообщество агентов основывается на принципах кооперации;

– структура сообщества агентов не исключает распределенность (размещение агентов на различных компьютерах), что позволяет эффективно организовать доступ к распределенным источникам данных;

– агенты используют в качестве предметной области для решения задач сбора и обработки медицинской статистики – федеральную базу ИЭМК и её распределённую копию;

– агенты обеспечивают работу в асинхронном режиме;

– появление новых членов сообщества агентов или изменение функций некоторых агентов не требует перезагрузки всей информационной системы;

– структура сообщества базируется на требованиях FIPA (Federation of Intelligent Physical Agents) [3].

МАПК СОМС представлен сообществом агентов, которые разделены на три группы в зависимости от основного назначения.

Первая группа агентов взаимодействует с внешней средой – потоком ЭПМЗ и запросов на данные из базы ИЭМК. Эта группа представлена координатором, помощником, а также агентом доступа к данным. Агент-координатор выполняет функцию верификации идентификационной части входного потока ЭПМЗ и запускает, в случае необходимости, технологические линии по присвоению соответствующих идентификаторов. Агент-помощник, опираясь на данные из онтологии, выполняет задачу поверки корректности запроса данных из базы ИЭМК и контроль достоверности запрошенных данных. Агенты координатор и помощник фактически определяют входной и выходной интерфейс МАПК СОМС и обеспечивают условия устойчивой работы агента доступа к данным. Данная группа агентов может естественным образом вносить свой вклад в дело формирования статистической картины здравоохранения, в частности, сохраняя данные о ежедневном количестве обслуженных пациентов, а также числе врачей и диагностических лабораторий, вовлечённых в лечебно-диагностический процесс на суточном интервале.

Вторая группа отражает декомпозицию задач СОМС и включает экспертов предметной области. Агент-эксперт вводится в систему для решения специфичных задач, основываясь на международной классификации болезней, то есть делается акцент на конкретную нозологию или врачебную специальность. Например, специальный агент сбора статистических данных о сердечно-сосудистых заболеваниях, не только ведёт количественный учёт этого класса заболеваний, но и должен пытаться определить особенные характеристики, в частности, удалось ли в конкретном лечебно-диагностическом процессе уложиться в «золотой час» при инсульте.

Третья группа занимается непосредственно вычислениями и объединяет агентов расчета агрегированных показателей, агентов корреляционного и регрессионного анализа. Эта группа агентов использует для вычислений не только данные из базы ИЭМК, но и данные сформированные агентами первой и второй групп. В частности, рассчитывая показатели рождаемости и смертности, соответствующие агенты строят и корректируют распределения не только по возрастным категориям и регионам, но и по нозологиям, используя информацию, созданную агентами второй группы.

Важным свойством инновационной системы сбора и обработки медицинской статистики должно стать не только оперативное определение (в режиме реального времени) статистических

характеристик лечебно-диагностических процессов, но и выработка сигнальных индикаторов, которые будут говорить о критических изменениях, требующих оперативного перераспределения ресурсов здравоохранения для борьбы с эпидемиями и стихийными бедствиями.

Кроме того, мы вправе ожидать от МАПК СОМС выработки сигналов о наличии признаков возникновения дефектов оказания медицинской помощи в рамках конкретного лечебно-диагностического процесса. К числу таких признаков, в частности, относится появление ЭПМЗ, в которой констатируется смерть пациента. В этом случае, независимо от наличия или отсутствия результатов патологоанатомического исследования, должен быть запущен анализ всей истории взаимоотношений данного пациента с системой здравоохранения.

Свободная лицензия для программного комплекса сбора и обработки медицинской статистической информации

Предлагая МАПК СОМС, как естественный (понятный, алгоритмически определённый) технологический этап развития информатизации здравоохранения на основе федеральной базы ИЭМК, следует ещё раз обратить внимание на юридический статус и перспективы постоянного совершенствования такого рода программ. Поскольку речь идёт о программах, результаты работы которых прямо или косвенно влияют на здоровье и саму жизнь пациентов и, в каком-то смысле, выполняют роль медицинских препаратов, то сокрытие алгоритмов и текстов программ следует считать делом недопустимым и даже аморальным.

В основу программ для здравоохранения должны быть положены принципы, которые обеспечат:

– безопасность и надежность программных средств;
– высокий уровень управляемости развитием программного обеспечения;
– масштабируемость и кроссплатформенность для всего разнообразия участников информационного процесса;
– юридическую защиту прав потребителей программных средств (врачей, диагностических лабораторий и пациентов);
– гарантию качества программных инструментов;
– экономию средств на внедрение и сопровождение данной информационной технологии;
– поддержка и развитие открытых стандартов.

Все эти свойства присущи свободному программному обеспечению (ПО) [7], [8].

Можно говорить о том, что осознание преимуществ свободного ПО для информатизации здравоохранения уже произошло. На конференции, посвященной электронной системе здравоохранения и телемедицине (eHealth & Telemedicine Philippines 2009 Conference and Exhibition), участники обратили особое внимание на важную роль свободного ПО и ПО с открытым кодом (FOSS) в развитии электронного медицинского документооборота. В сенате США рассмотрены предложения по созданию национальной медицинской информационной системы на базе открытого ПО. Предложен новый законопроект «Health Information Technology Public Utility Act of 2009», который предусматривает выделение федеральных грантов на разработку open source информационной системы и создание набора открытых стандартов для унифицированного учета медицинских карточек во всех медицинских учреждениях страны.

Для России, в текущих стеснённых экономических обстоятельствах, тем более важно, выделяя значительные средства на программные проекты в сфере здравоохранения, законодательно определить реализацию этих продуктов в виде свободного ПО и ПО с открытым кодом. Это позволит не тратить средства на многократную реализацию одних и тех же алгоритмов, а закладывать в бюджет разумные средства на модернизацию существующего свободного ПО, обеспечивая при этом здоровую конкуренцию в среде разработчиков.

Одним из важных следствий разработки МАПК СОМС должна стать отработка технологии ведения федерального репозитория версий программных агентов с сохранением, в том числе, открытого программного кода, доступного, как для верификации, так и для модернизации, которую могут выполнить не только первоначальные разработчики программного продукта.

Заключение. Информатизация здравоохранения, к сожалению, остается социальным процессом, который, как и само здравоохранение, финансируется по остаточному принципу. Эта объективная реальность вынуждает выбирать те инновационные проекты, которые, во-первых, актуальны и алгоритмически проработаны, во-вторых, имеют очевидный экономический эффект и, наконец, создают технологические заделы для решения очередных, более сложных задач информатизации здравоохранения. К числу таких проектов, безусловно, следует отнести проект разработки инновационной программной государственной системы сбора и обработки медицинской статистики на основе данных федеральной базы ИЭМК.

СПИСОК ЛИТЕРАТУРЫ

1. Wooldridge M. An Introduction to MultiAgent Systems. Wiley, 2009.
2. Shamma Jeff. Cooperative Control of Distributed Multi-Agent Systems. John Wiley & Sons, 2008.
3. Bordini R.H., Dastani M., Dix J., Seghrouchni A. Multi-Agent Programming: Languages, Tools and Applications. Springer, 2009.
4. Куракова Н.Г. Информационные системы и технологии в здравоохранении. Главврач, 2003, №7, С.58–59.

5. Ермаков С.П. Лукавые цифры: так ли успешно снижается смертность в России, http://www.slideshare.net/KomitetGI/ss-42639205
6. Гусев А.В. Состав статистической информации, собираемой в отечественном здравоохранении. http://www.gosbook.ru/node/87357
7. **Блюм В.С., Заболотский В.П.** Свободное программное обеспечение для здравоохранения // Труды СПИИРАН, 2009, Вып. 8, С. 46–60.
8. Блюм В.С. Технология обработки первичной медицинской информации для раннего обнаружения врачебных ошибок. Математическая морфология. Электронный математический и медико-биологический журнал, Т.9, Вып. 4, 2010.
9. Блюм В.С. Ообенности биологических систем информационной безопасности. Математическая морфология. Электронный математический и медико-биологический журнал, Т.13, Вып. 1, 2014.
10. Блюм В.С., Заболотский В.П. Социальная иммунная система и ммунокомпьютинг. Математическая морфология. Электронный математический и медико-биологический журнал, Т.13. Вып. 1, 2014.
11. Блюм В.С. Дскретно-событийная модель здравоохранения и федеральный сервис «интегрированная электронная медицинская карта». Математическая морфология. Электронный математический и медико-биологический журнал, Т.11, Вып. 4, 2012.
12. Блюм В.С., Заболотский В.П. Базовое программное обеспечение для здравоохранения / Математическая морфология. Электронный математический и медико-биологический журнал, Том 8, вып. 3, 2009. Идентификационный номер 0420900004\0027.

УДК 502.084

КЛАССИФИКАЦИЯ ПРОГРАММНЫХ АГЕНТОВ ДЛЯ РАННЕГО ОБНАРУЖЕНИЯ ДЕФЕКТОВ ОКАЗАНИЯ МЕДИЦИНСКОЙ ПОМОЩИ ПО ДАННЫМ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ

Блюм Владислав Станиславович, Заболотский Вадим Петрович,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия В.О., 39,
e-mails: vlad@blum.spb.su, lai@iias.spb.su

Аннотация: Чрезвычайная сложность человеческого организма и ограниченность знаний о его функционировании приводит к тому, что любая, даже самая развитая, система здравоохранения обречена на значительный (по данные ВОЗ не менее 10%) процент дефектов оказания медицинской помощи в общем числе оказанных медицинских услуг. Поэтому раннее обнаружение дефектов оказания медицинской помощи всегда было и остаётся одной из наиболее актуальных и острых проблем в сфере здравоохранения. Качественные изменения в способах решения указанной проблемы наметились в связи с переходом на электронный способ формирования персональных медицинских записей врачами и диагностическими лабораториями, а также с перспективами интегрирования электронных медицинских карт в региональных и федеральном центре. Появление региональных и федеральной баз интегрированных электронных медицинских карт позволяет ставить задачу разработки системы программных агентов, нацеленных на непрерывный анализ потока первичной медицинской информации для обнаружения всех видов нарушений медицинского технологического процесса. В статье приведена иерархия указанного множества программных агентов.

Ключевые слова: *Информатизация здравоохранения; дефекты оказания медицинской помощи; интегрированная электронная медицинская карта.*

CLASSIFICATION OF SOFTWARE AGENTS FOR EARLY DEFECT DETECTION OF MEDICAL CARE BASED ON INTEGRATED HER

Blum Vlad, Zabolotski Vadim,
St. Petersburg, Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg 14 line V.O., 39
e-mails: vlad@blum.spb.su, lai@iias.spb.su

Abstract: The complexity of the human body and the limited knowledge about its functioning leads to the fact that any, even the most advanced health care system is doomed to a significant (at least 10% – WHO data), the percentage of defects of medical care in the total number of rendered medical services. Therefore, early detection of defects in health care has always been and remains one of the most urgent and pressing problems in health care. Qualitative changes in the methods of solving this problem emerged in connection with the transition to an electronic method of forming personal medical records by physicians and diagnostic laboratories, as well as to the prospects of integration of electronic medical records in the regional and the federal center. The emergence of regional and federal databases integrated electronic health record allows us to pose the challenge of developing system software agents aimed at continuous flow analysis of primary medical information to detect all kinds of medical disorders of the process. This article is an attempt to classify the plurality of software agents.

Keywords: *Computerization of health; defects care; integrated electronic medical record.*

Введение. В последние годы активизировался процесс перехода от рукописной фиксации первичной медицинской информации (записей врачей и отчётов диагностических лабораторий) к их электронным образам – электронным персональным медицинским записям (ЭПМЗ). Более того, сделаны заметные шаги в направлении сбора ЭПМЗ в интегрированных электронных медицинских картах, для которых созданы (и создаются) базы данных в региональных и федеральном центрах обработки данных (ЦОД). Таким образом, появляется реальная перспектива получения полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации необходимой и достаточной для решения качественно новых задач поддержки врачебной деятельности и управления здравоохранением.

Особый интерес, с точки зрения перспектив использования объективных, достоверных данных об оказании лечебно-диагностической помощи населению для математического моделирования и решения актуальных задач практического здравоохранения (задача выживаемости, задача раннего обнаружения дефектов оказания медицинской помощи и т.д. и т.п.), вызывает реализация проекта федерального сервиса «Интегрированная электронная медицинская карта».

Проект грандиозный, поскольку ещё десять лет тому назад сбор и обработка подобного потока сложной информации, источники которой разбросаны по всей стране, был технологически не реализуем. Годовой объём первичной медицинской информации составляет 3–5 терабайта [1], с интенсивностью более миллиона персональных медицинских записей в сутки, при большом структурном разнообразии и высокой семантической сложности.

Перспектива создания этого интегратора открывает возможность и необходимость разработки систем программных агентов, способных оказывать реальную информационную поддержку врачу и уберечь тысячи пациента от неминуемых врачебных ошибок, одновременно порождая большой объём необходимой для управления статистической информации. Программный агент – это программа, которые не запускаются непосредственно для решения задачи, а активизируются самостоятельно.

Для разработки такой системы программных агентов необходимо выполнение ряда предусловий их эффективной работы. Помимо развития телекоммуникационной инфраструктуры, к числу этих предусловий следует отнести ещё два класса программ, которые будут рассмотрены в предлагаемой классификации.

Федеральный сервис «Интегрированная электронная медицинская карта»

Согласно техническому заданию на создание первой очереди интегрированной электронной медицинской карты и сервисов доступа к ней [http://zakupki.gov.ru], работы, по внедрению интегрированной электронной медицинской карты и сервисов доступа к ней, должны быть реализованы с использованием сервисно-ориентированных и облачных технологий, входящей в состав Единой государственной информационной системы в сфере здравоохранения Российской Федерации. В техническом задании указано, что «основной целью ведения Интегрированной электронной медицинской карты (далее ИЭМК) является обеспечения непрерывности, преемственности и качества лечения, а также своевременной профилактики и иных мероприятий по обеспечению здоровья конкретного индивида путем документирования и сохранения соответствующей медицинской информации и своевременного предоставления ее уполномоченным медицинским работникам и организациям, а также субъектам ИЭМК.»

Главным эффектом от внедрения ИЭМК должна стать качественно новая электронная история болезни (ЭИБ), в которой будут учтены все встречи пациента с системой охраны здоровья. Такая ЭИБ будет доступна для анализа и принятия обоснованных решений с гораздо большей оперативностью за счёт централизованной программной обработки в региональных и федеральном ЦОД.

ИЭМК – это коллекция ЭПМЗ, которая включает все, без исключения, упорядоченные по времени медицинские записи, относящиеся к конкретному пациенту независимо от того, в каком ЛПУ или лаборатории страны они выполнены.

Электронная история болезни и персональная электронная медицинская запись

Электронная история болезни (ЭИБ) согласно ГОСТ [ГОСТ Р 52636-2006] – это «информационная система, предназначенная для ведения, хранения на электронных носителях, поиска и выдачи по информационным запросам (в том числе и по электронным каналам связи) персональных медицинских записей.» ЭИБ состоит из размещённых в хронологической последовательности электронных персональных медицинских записей (ЭПМЗ). Понятие «электронная персональная медицинская запись» соответствует международному термину EHR – Electronic Health Record [1].

В системе здравоохранения существует два класса легитимных источников «производства» ЭПМЗ – это дипломированные (сертифицированные, лицензированные, аттестованные) врачи и

лицензированные диагностические лаборатории (ДЛ). Ежедневно в России производится около миллиона таких записей [1].

Синтаксическая структура ЭПМЗ на метаязыке может быть представлена в виде:

<ЭПМЗ ВРАЧА> ::= <время сеанса>< идентификатор ВРАЧА>< идентификатор ПАЦИЕНТА>< документ ВРАЧА> (1)

<ЭПМЗ ДЛ> ::= <время сеанса>< идентификатор ДЛ>< идентификатор ПАЦИЕНТА>< документ ДЛ.> (2)

Временно исключим из рассмотрения множество ЭПМЗ диагностических лабораторий на том простом основании, что в записях врача с необходимостью присутствует оценка результатов лабораторных исследований.

Обратим внимание на два обязательных атрибута ЭПМЗ, на <время сеанса> и < идентификатор ПАЦИЕНТА>.

Обозначим ЭПМЗ, сделанную j-м врачом по поводу i-го пациента, как $z(i,j,t)$, где t – время, указанное в ЭПМЗ, а соответствующее событие обозначим как – $\breve{z}(i,j,t)$. Выделим два особых вида ЭПМЗ и соответствующих событий: записи, в которых врач фиксирует появление (рождение) нового пациента, обозначим – $z_0(i,j,t)$, а записи, в которых врач констатирует смерть пациента, обозначим – $z_f(i,j,t)$. Эти события обозначим как $\breve{z}_0(i,j,t)$, $\breve{z}_f(i,j,t)$.

Идентификация электронной истории болезни

Поскольку именно врач принимает решение о факте рождении и смерти, то можно сделать первый вывод: система здравоохранения не нуждается в такого рода информации от отделов ЗАГС и других органов государственной власти для организации собственного документооборота. Более того, возникновение в системе новой записи $z_0(i)$ о рождении пациента, при условии централизованного учёта, может быть использовано для формирования уникального идентификатора истории болезни нового i-го пациента. Для этого достаточно использовать знания о среднем числе рождений в сутки и определить разрядность счётчика: для Петербурга достаточно трёхразрядного числа (около 150 рождений в сутки), для России в целом – четырёхразрядного счётчика (порядка 5 000 рождений), для Всемирной организации здравоохранения (ВОЗ) – семиразрядного числа.

В этом случае, уникальный идентификатор интегрированной электронной медицинской карты будет иметь вид:

<Идентификатор ИЭМК> ::= <дата рождения><учётный номер в системе здравоохранения> (3)

Предложенный способ идентификации задаёт отношение строгого порядка на множестве ИЭМК. Тогда областью значений грамматической категории <Идентификатор ИЭМК> будет множество нумерованных дат рождения пациентов, а идентификатор i -го пациента – значение функции $I(z_0(i)) = I_{0i}$, для $\forall i$, где I_{0i} – уникальный идентификатор пациента, на основании которого определяется возраст пациента относительно текущего момента времени.

Для $\forall i,j \quad I_{0i} > I_{0j}$ или $I_{0i} < I_{0j}$.

В этом случае, конечное множество идентификаторов ИЭМК ($ID = \{I_{01}, I_{02}, ..., I_{0n}\}$) может быть упорядочено на временной оси и интерпретироваться, как множество моментов времени, которые фиксируют события рождения пациентов. При таком подходе текущий момент времени – t_0 и идентификатор ИЭМК определяют реальный возраст пациента. Для заданного множества идентификаторов ИЭМК всегда может быть найдена карта самого возрастного пациента, не содержащая записи $z_f(i)$ – запись о смерти пациента. Такой идентификатор обозначим как – I_{0s}.

Интервал времени $\Delta = t_0 - I_{0s}$ назовём актуальным интервалом времени жизни популяции. Ось времени, на которой размещены моменты рождения пациентов, назовём осью времени жизни популяции и обозначим – t_ρ. Ясно, что на интервале Δ зафиксированы моменты рождения не только пациентов, требующих текущего внимания системы охраны здоровья, но и тех, в истории болезни которых имеется ЭПМЗ – $z_f(i)$. Такие ЭИБ будем считать закрытыми, но не потерявшими своего информационного значения для системы здравоохранения. Обозначать такие ИЭМК будем как $\widehat{I}_{0i}$. А событие, связанное с появлением ЭПМЗ о рождении нового пациента обозначим – $\breve{I}_{0i}$.

Предложенный способ идентификации ИЭМК и её составляющих – ЭПМЗ, имеет ряд технологических преимуществ по сравнению с любым другим способом. Психологически пациенту легко запомнить код своей электронной медицинской карты – это всего пять цифр, кроме даты рождения. Факт рождения нового пациента фиксируется именно системой здравоохранения и

фиксируется раньше, чем гражданин обретает имя. Оперативный централизованный учёт нового пациента становится реальной и просто решаемой задачей в связи с переходом на электронный документооборот в здравоохранении и созданием для этих целей федерального центра обработки данных (ЦОД).

Как уже указывалось, предложенный способ идентификации задаёт отношение строго порядка на множестве всех пациентов и их ИЭМК. Более того, введение в учётную схему нового пациента любого возраста не нарушает этот строгий порядок и технологически не сложен, так как процедура связана с простым добавлением очередной записи в границах учётной даты. Таким образом, предложенный способ идентификации ИЭМК позволит однозначно связать конкретного пациента с каждой, выполненной по поводу его здоровья ЭПМЗ, с его электронной медицинской картой в конкретном лечебно-профилактическом учреждении и, наконец, с его ИЭМК в региональном и федеральном ЦОД.

Для реализации программной поддержки данного способа идентификации пациентов необходима соответствующая технология. Технология идентификации ИЭМК включает ряд программных агентов в федеральном ЦОД и программы идентификации и верификации имени ИЭМК пациента, работающей в каждом ЛПУ и диагностической лаборатории.

В программные агенты, поддерживающие технологию идентификации документов в базе ИЭМК ЦОД, входят:

1. Программа контроля входного потока ЭПМЗ.
2. Диалоговая программа регистрации новой ИЭМК.
3. Программа закрытия ИЭМК.

Программа идентификации и верификации ИЭМК пациента, которой должны быть оснащены все ЛПУ, инициируется источником ЭПМЗ, если необходимо создать новую ИЭМК, либо запускается программно по инициативе программного агента ЦОД, если отправленная в ЦОД ЭПМЗ не находит свою ИЭМК.

Событийная модель базы ИЭМК

Для построения событийной модели базы ИЭМК [3] определим ортогональную систему координат, в которой осью абсцисс станет t_ρ – дискретная ось времени жизни популяции, а осью ординат будет непрерывная временная ось, которую назовём осью времени жизни пациентов и обозначим – t_τ. Начало координат определим, как самый ранний момент времени рождения пациента, история болезни которого, по каким-то причинам, сохранилась в архивах системы здравоохранения (рисунок 1), но так, чтобы все наши дальнейшие построения выполнялись в первом квадранте построенной системы координат.

Для самого возрастного пациента, идентификатор ИЭМК которого – I_{0s}, построим вектор $\vec{v}_{0s}$, длина которого $|\vec{v}_{0s}|$ будет равна реальному времени жизни этого пациента. Вектор $\vec{v}_{0s}$ разместим параллельно оси t_τ с началом в точке I_{0s}. Очевидно, что $|\vec{v}_{0s}| = \Delta$ – время жизни пациента равное времени жизни популяции.

Покажем, что вектор $\vec{v}_{0s}$ есть проекция информационного вектора истории болезни на временную ось t_τ.

Построим соответствующие вектора $\vec{v}_{0i}$ для всех учтённых ИЭМК (имеющих идентификаторы – I_{0i}), но не имеющих ЭПМЗ – $z_f(i)$. Начало этих векторов будет лежать на оси t_ρ, а конец окажется одной из точек гипотенузы равнобедренного прямоугольного треугольника с катетом $|\vec{v}_{0s}|$.

Каждый из построенных векторов суть временной образ (проекция) информационного вектора истории болезни конкретного пациента, который, в свою очередь, состоит из суммы векторов, число которых соответствует числу ЭПМЗ в данной ИЭМК.

$\vec{v}_{0i} = \sum_{j=1}^{k} \vec{v}_j$, где k – число записей в ИЭМК i-го пациента, а $|\vec{v}_j|$ – интервал времени от данной ЭПМЗ до следующей, либо до текущего момента t_0. Заметим, что текущий момент времени рассматриваемом в пространстве $T \times T$ характеризуется прямой $y = -t + t_0$.

Прямоугольный треугольник, катетами которого являются вектор $\vec{v}_{0s}$ и отрезок оси t_ρ – $[I_{0s}, t_0]$, ограничивает временное пространство $\Omega \subset T \times T$, в котором размещены все, без исключения, актуальные события, которые фиксируют моменты возникновения ЭПМЗ вида (1) в системе здравоохранения (системе ныне здравствующих пациентов). Актуальными будем называть такие

события, которые соответствуют ЭПМЗ здравствующих пациентов, то есть пациентов, в ИЭМК которых не содержится записи – $z_f(i)$.

Таким образом, мы построили ограниченное временное пространство Ω, в котором размещены и строго упорядочены ЭПМЗ всех ныне здравствующих потенциальных пациентов (рисунок 1).

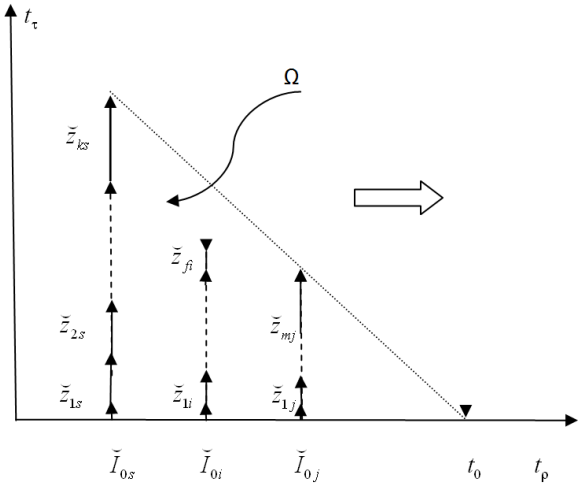


Рис. 1. Модель событий базы ИЭМК

В данной модели для текущего момента t_0 векторные образы ИЭМК всех учтённых живых пациентов упорядочены по величине (времени жизни пациента), а вершины всех векторов лежат на одной прямой, которая является гипотенузой прямоугольного треугольника, ограничивающего временное пространство Ω. В пространстве $\Omega \subset T \times T$ размещены и строго упорядочены по оси t_ρ все ИЭМК, а по оси t_τ строго упорядочены все ЭПМЗ в векторах каждого пациента.

Гипотенуза равностороннего треугольника (пространства Ω) – это отрезок прямой $y = -t + t_0$, длиной $\sqrt{2}\left|\vec{v}_{0s}\right|$. Особенностью этого отрезка является то, что он определяет интерфейс системы здравоохранения. Именно на этом ограниченном отрезке, и только на нём, могут возникнуть новые события (ЭПМЗ) в данной модели системы охраны здоровья в текущий момент времени.

Алгоритм функционирования модели событий базы ИЭМК

Выбирая шаг h для наблюдения за динамикой развития модели событий базы ИЭМК, очевидно, речь идёт о суточном интервале, необходимо определить алгоритм учёта новых событий и исключения из рассмотрения не актуальных ИЭМК. Понятно, что правила внесения изменений в модель не должны приводить к временным коллизиям.

Пусть $h = t_1 - t_0$. Тогда, прямая $y = -t + t_0$ примет вид $y = -t + t_1 + h$, где $t_0 = t_1 + h$ текущий момент времени (рис.3). Прямые $y = -t + t_0$ и $y = -t + t_1$ задают временное окно, в котором разрешены новые события (возникновение новых ЭПМЗ) в системе здравоохранения. Пространство Ω потенциально увеличивается на величину $\frac{h}{2}(2\Delta + h)$.

Для приведения модели в соответствие с текущим временем t_0 должны быть выполнены следующие операции.

Выделение вычислительных ресурсов для ИЭМК новых пациентов, родившихся на интервале h, т.е.формирование новых идентификаторы $I_{0t_1}, I_{0t_2}, \ldots, I_{0t_n}$ в порядке поступления n заявок (записей $z_{0t_1}, z_{0t_2}, \ldots, z_{0t_n}$).

Для сохранения возможности фиксации точного времени новых событий в группе ИЭМК – $I_{0t_1}, I_{0t_2}, \ldots, I_{0t_n}$ на интервале h, соответствующие вектора назначаются равными $\vec{h}$.

Каждый вектор $\vec{v}_{0i}$, за исключением векторов новорождённых, увеличивается до пересечения с $y = -t + t_0$, причем

– – если на интервале h пациент i не встречался врачом, то

– $\vec{v}_{0i} + \vec{h} = \vec{v}'_{0i}$ и $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{h}|$, но k – число записей в ИЭМК i -го пациента к моменту t_0 не изменяется;

– – если на интервале h пациент i имел одну или более встреч с врачом, то

– $\vec{h} = \vec{v}_{0i_1} + \vec{v}_{0i_2} + ... + \vec{v}_{0i_m}$, где m – число ЭПМЗ i -го пациента на интервале h и

– $\vec{v}_{0i} + \vec{h} = \vec{v}'_{0i}$ и $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{h}|$, но k – число записей в ЭИБ i -го пациента к моменту t_0 увеличивается на величину m.

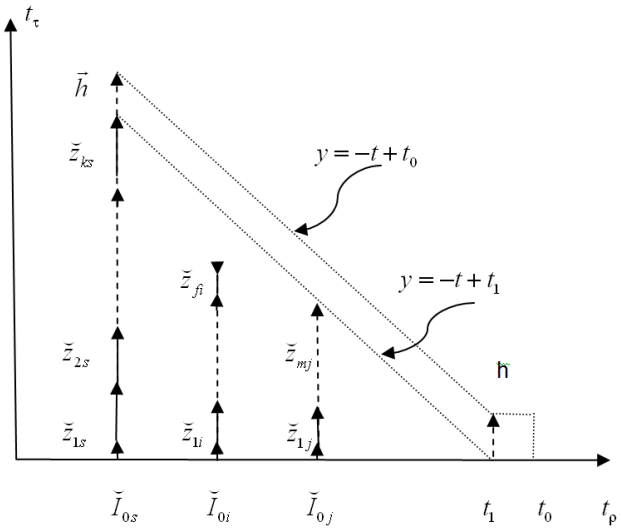


Рис. 2. Динамика событий в модели базы ИЭМК

1. Если на интервале h для i -го пациента возникает запись $z_f(i)$ (вектор – $\vec{v}_{fi}$), то ИЭМК закрывается, обозначим её как $I_{0i} = [I_{0i}]$,а вектор $\vec{v}_{0i}$ обращается в скаляр $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{v}_{fi}|$.

2. Если на интервале h для s -го пациента (самого возрастного) возникает запись $z_f(i)$, то выполняется коррекция (уменьшение) пространства Ω. Для этого в списке идентификаторов ИЭМК определяется такой не закрытый I_{0i}, что $\Delta = t_0 - I_{0i} = \max$. Для выбранного идентификатора ИЭМК I_{0i} фиксируется статус I_{0s}.

– вычисляются характеристики пространства Ω на момент времени t_0:

– число актуальных историй болезни (число живых пациентов);

– число закрытых ИЭМК на интервале h (число умерших в текущие сутки);

– коэффициент выживаемости для пространства Ω, а также для любой заданной возрастной категории пациентов (отношение числа актуальных ИЭМК к общему числу учтённых ИЭМК);

– и другие технологические операции и статистические оценки.

Рассмотренный алгоритм указывает на то, что формирование полной, достоверной и доступной для обработки базы ИЭМК предполагает наличие нового класса программных агентов, выполняющих непрерывное обслуживание потока ЭПМЗ в региональных и федеральном ЦОД.

В состав этих агентов входят:

1. Программа контроля разрешённого интервала изменений.
2. Программа коррекции пространства событий.
3. Программа коррекции информационного вектора ИЭМК при отсутствии событий на данном интервале.
4. Программа расчёта статистических данных на заданном интервале.
5. Программа коррекции интегральных статистических характеристик актуального пространства событий.
6. Программа коррекции актуального списка пациентов.

Информационная модель базы ИЭМК

Интегрированная электронная медицинская карта это сумма векторов – ЭПМЗ, которая пополняется системой охраны здоровья на протяжении всей жизни пациента. Начиная с момента рождения, система здравоохранения производит персональные медицинские записи (теперь – ЭПМЗ)

и последовательно размещает их в истории болезни (теперь – ИЭМК). Каждая запись имеет собственное информационное наполнение. Не пытаясь на этом этапе оценивать семантику записи, мы всегда можем посчитать количество бит, необходимых для хранения данной ЭПМЗ в памяти компьютера. Ясно, что каждый бит такой записи, в той или иной степени несёт в себе информацию о ресурсах затраченных системой здравоохранения на данного пациента. Очевидно, что каждый вектор (ЭПМЗ) имеет фиксированную по величине (количеству бит) проекцию на информационно-временную плоскость $I \times T_\rho$ (см. рисунок 3).

Особенность предлагаемой информационной модели базы ИЭМК заключается в том, что, при сохранении неизменной величины проекции вектора ЭПМЗ на плоскость $I \times T_\rho$ (в записи не добавляется битов), его проекция на плоскость $I \times T_\tau$ непрерывно увеличивается до момента появления очередной ЭПМЗ, что характеризует процесс старения информации.

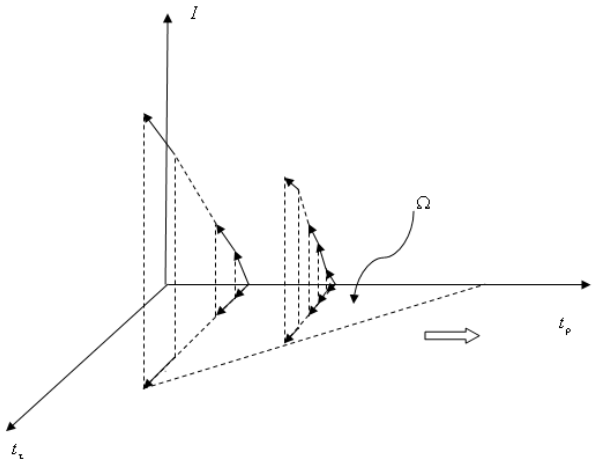


Рис. 3. Информационная модель базы ИЭМК

Вектор последней записи (ЭПМЗ) будет изменять величину и угол наклона к плоскости $I \times T_\tau$ вплоть до появления очередной записи.

Каждая ИЭМК размещена в персональной для данного пациента информационно-временной плоскости ($I \times T$), которая характеризуется моментом рождения – I_{0i} (рисунок 3).

В результате анализа информационного вектора ИЭМБ, может быть оценено не только его информационное наполнение (объём ресурсов здравоохранения, затраченных на пациента), но и, так называемый, «угол внимания» системы здравоохранения по отношению конкретному пациенту. Этот параметр важен при организации государственной системы диспансерного контроля состояния здоровья.

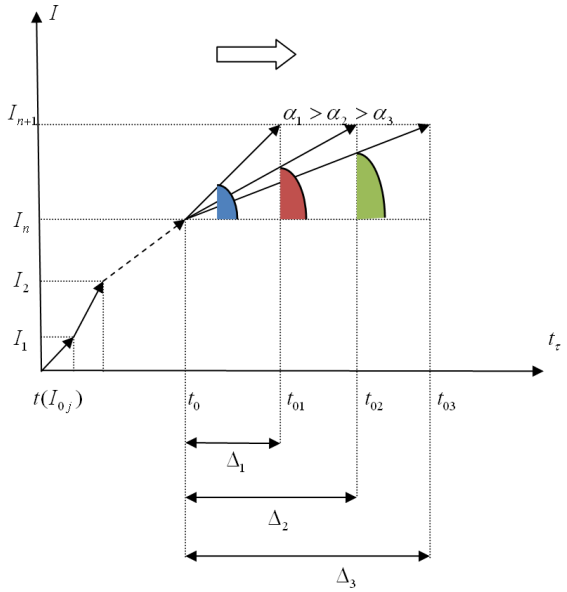


Рис. 4. Информационный вектор истории болезни

Рассмотрение персональной информационно-временной плоскости ИЭМК показывает, что при увеличении интервала времени между возникновениями двух последовательных ЭПМЗ $\Delta_1 < \Delta_2 < \Delta_3$ уменьшается угол наклона информационного вектора $\alpha_3 < \alpha_2 < \alpha_1$, что может быть использовано в качестве объективного критерия для учёта «оторвавшихся» от диспансерного наблюдения и организации профилактического контроля здоровья с учётом всей предыстории врачебных вмешательств.

Информационная составляющая ЭПМЗ является объектом семантического анализа. В частности, грамматическая категория <документ врача>, как правило, раскрывается раскрывается через следующие грамматические категории:

<документ врача>::=<жалобы><анамнез><диагноз><назначения>

Предполагает создание класса программных агентов, нацеленных на оперативную оценку эффективности использования ресурсов здравоохранения и раннее обнаружение дефектов оказания медицинской помощи по данным из базы ИЭМК.

В состав этого класса программных агентов следует включить следующие программы:

1. Программа персонифицированной оценки объёма и оценки целесообразности затраченных ресурсов здравоохранения.
2. Коллекция программ оценки эффективности персонифицированного лечебно-диагностического процесса по нозологиям.
3. Коллекция программ сравнительного анализа лечебно-диагностических процессов по нозологиям.
4. Программа контроля интервалов диспансерного обследования
5. Программа анализа события смерти пациента
6. Коллекция программ проверки известных дефектов оказания медицинской помощи.
7. и другие программы семантической обработки ИЭМК

Иерархия программных агентов мониторинга врачебной деятельности

Анализ формальной событийной модели базы ИЭМК, которая нацелена на хранение полного, достоверного и доступного для автоматизированной обработки потока первичной медицинской информации, указывает на то, что для функционирования и эффективного использования этой базы данных должны быть реализованы взаимообусловленные коллекции программных агентов, то есть программы, которые выполняют непрерывный мониторинг состояния базы ИЭМК и поддерживают её функционирование.

Можно выделить следующие классы программных агентов:

1. Класс программных агентов, поддерживающих технологию идентификации документов в базе ИЭМК ЦОД.
2. Класс программных агентов, реализующих алгоритм функционирования модели базы ИЭМК.
3. Класс программных агентов оперативной статистической оценки интенсивности лечебно-диагностического процесса – характеристики информационного потока ЭПМЗ для различных регионов и ЛПУ.
4. Класс программных агентов, поддерживающих решение задач статистической и семантической обработки информации в базе ИЭМК для раннего обнаружения дефектов оказания медицинской помощи и управления лечебно-диагностическим процессом.

Рис. 5. Иерархия программных агентов над базой ИЭМК

Построение такой иерархии программных агентов предполагает изменение статуса электронной истории болезни. Каковы пути повышения статуса ЭМК в системе здравоохранения?

На наш взгляд, существует простое технологическое решение для ответа этот вопрос.

С этой целью необходимо директивно обязать (например, внесением изменений в ФЗ №326-ФЗ) все существующие и перспективные МИС, при сохранении электронной персональной медицинской записи (ЭПМЗ) в базе МИС (если, конечно, такую работу выполняет данная МИС), отправлять эту запись в федеральную (или региональную) базу интегрированных ЭМК (ИЭМК).

Очевидно, что такая директива не станет дополнительной нагрузкой для лечебно-диагностического процесса. Это чрезвычайно важно [5]! Начальным мотивом может быть стать оптимизация (минимизация) структуры системы сбора и обработки медицинских статистических данных на основе создания соответствующего программного обеспечения в федеральном ЦОД.

Такая целевая установка может на время ослабить требования к защите персональных данных, поскольку пользователями информации назначаются исключительно программные комплексы. Экономический эффект от создания новой системы статистического учёта и обработки данных из базы ИЭМК, думаю, очевиден.

Решение задачи сбора и обработки математической статистики на основе данных их базы ИЭМК и предложенной модели будет способствовать решению таких базовых проблем, как:

1. Идентификация источников ЭПМЗ и формирование актуального реестра врачей и диагностических лабораторий.
2. Идентификации пациентов и их уникальных ИЭМК.
3. Развитие телекоммуникационной инфраструктуры системы здравоохранения и электронных хранилищ первичной медицинской информации.
4. Отработка структур ЭПМЗ для их эффективной автоматизированной обработки.

Главный результатом должно стать появление полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации в федеральном ЦОД, в форме базы ИЭМК, дополненной актуальной статистической информацией.

С реализацией указанной, взаимообусловленной иерархии программных агентов над федеральной базой ИЭМК будет сделан решительный шаг в то светлое будущее, когда за плечом каждого врача окажется «искусственный интеллект» способный уменьшить число дефектов оказания медицинской помощи с 10% хотя бы до 5%, а принцип диспансерного наблюдения из разряда пожеланий будет переведён в практическую плоскость.

Заключение. Рассмотренная иерархия программных агентов над базой ИЭМК показывает реальный путь к качественному повышению эффективности системы здравоохранения при переходе от бумажного к электронному документообороту.

Важным шагом в этом направлении должно стать директивное направление потока полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации в федеральный ЦОД (например, внесением изменений в ФЗ №326-ФЗ), т.е. обязать все существующие и перспективные МИС, при сохранении электронной персональной медицинской записи (ЭПМЗ) в базе МИС (если, конечно, такую работу выполняет данная МИС), отправлять каждую вновь созданную запись в федеральную (или региональную) базу интегрированных ЭМК (ИЭМК).

СПИСОК ЛИТЕРАТУРЫ

1. Блюм В.С., Заболотский В.П. Мысленный эксперимент по организации учета и обработки информационных медицинских услуг. Врач и информационные технологии, №4, 2009, с.27–35.
2. Международный стандарт. ISO/TR 20514:2005. Информационные технологии в медицине – Электронная медицинская запись – Определение, назначение, содержание (Healthinformatics – Electronichealthrecord – Definition, scopeandcontext).
3. Рыжиков Ю.И. Имитационное моделирование. Теория и технологии. СПб.: КОРОНА принт.; М.: Альтекс-А, 2004.
4. В.М. Тавровский. Автоматизация лечебно-диагностического процесса.ООО «Вектор Бук». Тюмень, 2009, 464 стр.
5. Тавровский В.М., Гусев А.В. К чему должна привести информатизация здравоохранения. Попытка спроектировать будущее. Врач и информационные технологии, 2011, №5, С.60–70.

УДК 004.001.89

СОЗДАНИЕ СТРУКТУРЫ ИНТЕЛЛЕКТУАЛЬНОЙ ЭКСПЕРТНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ АНАЛИЗА МЕДИКО-БИОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ

Инкин Виталий Анатольевич, Делакова Екатерина Александровна,
Санкт-Петербургский Государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская 67,
e-mails: inkvitalya@mail.ru, ekaterina.delakova@gmail.com

Аннотация: В статье рассмотрена разработка структуры интеллектуальной системы поддержки принятия решений для анализа медико-биологических исследований, на основе применения процедур интеллектуального анализа многомерных данных. Так же была решена задача

кластеризации исследуемых данных с помощью программного обеспечения Rapid Miner, а так же сформирована предсказательная модель для сроков поверхностного заживления.

Ключевые слова: *Интеллектуальный анализ данных; классификация; кластеризация; анализ данных; регрессионная модель.*

THE DESIGN OF THE EXPERT DATA MINING DECISION SUPPORT SYSTEM FOR BIOMEDICAL RESEARCH ANALYSIS

Inkin Vitaliy Anatolyevich, Delakova Ekaterina Alexsandrovna,
St. Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya 67,
e-mails: inkvitalya@mail.ru, ekaterina.delakova@gmail.com

Abstract: The article presents the design of the expert data mining decision support system for biomedical research analysis based on multivariate data mining procedures. The data analyzed was clustered using Rapid Miner software; the predictive model was formed for superficial repair timeframe.

Key words: *data mining; classification; clustering; data analysis; regression model.*

В настоящее время информатизации здравоохранения, как важнейшему направлению модернизации и повышения эффективности управления и качества медицинской помощи, уделяется самое пристальное внимание. С точки зрения использования информационных технологий, медицина имеет огромный потенциал для внедрения и развития новых технологических решений для автоматизации процессов обследования и лечения пациентов.

Результатом развития информационных технологий является колоссальный объем данных, накопленных в электронном виде, растущий быстрыми темпами. Методы традиционной математической статистики долгое время претендовали на роль основного инструмента анализа данных. Однако, применение статистических методов целесообразно только при проверке заранее сформированной гипотезы, выявление и познание скрытых явлений, распознавание не очевидных закономерностей, моделирование изучаемых процессов предполагают обращение к более сложным методам анализа. В данной статье представлены результаты исследования математического аппарата интеллектуальной системы поддержки принятия решения врача на примере результатов обследования стоматологических пациентов. Функциональный базис системы – модель для прогноза продолжительности терапии пациентов с хронической и интактной травмой слизистой оболочки полости рта и губ (СОПР) [1].

Постановка задачи. В рамках данной работы были проведены: предварительный анализ ретроспективных данных результатов обследования стоматологических пациентов с целью выявления системы наиболее информативных признаков, обеспечивающих повышение качества принятия решений по прогнозированию сроков терапии пациентов; выбор математической модели для кластеризации пациентов и разработка математических моделей принятия решений по прогнозированию продолжительности терапии пациентов.

Материалы и методы. Известно, что слизистая оболочка полости рта (СОПР) – одна из важнейших систем организма, осуществляющая барьерную функцию в отношении действия патогенных биологических, физических и химических факторов. Состояние слизистой оболочки полости рта является индикатором тяжести патологических процессов, иммунного статуса, а также общего уровня активности и биологического состояния организма. Исследование состояния данной системы является актуальным для повышения качества диагностики состояния здоровья пациентов.

Сбор данных и клинические эксперименты проводились на базе поликлиники №23 Санкт-Петербурга, являющейся клинической базой кафедры пропедевтики стоматологических заболеваний Санкт-Петербургского государственного медицинского университета им. акад. И.П. Павлова. В исследование по определению возрастных морфофункциональных особенностей интактной и травматизированной СОПР и губ были включены 800 пациентов в возрасте от 20 до 79 лет.

В клиническое и лабораторно-инструментальное обследование пациентов входило изучение анамнеза жизни, заболевания, общего и локального стоматологического статуса пациентов. Для каждого пациента была собрана информация о морфологическом состоянии СОПР, а также мы располагали данными о патологическом состоянии пациентов и о применяемых препаратах. К тому же для каждого пациента, принимавшего участие в исследовании, указана информация о статусе здоровья, индексе гигиены, наличии или отсутствии сердечно-сосудистых патологий (ишемическая болезнь сердца (ИБС), вегетососудистая дистония (ВСД) по гипертоническому типу) и патологий желудочно-кишечного тракта (хронический гастрит).

В общем случае для анализа мы располагали более 40 показателями для каждого пациента. В качестве целевого параметра была выбрана скорость заживления травматических деформаций в полости рта и оперативность реакции пациента на проводимое лечение.

Для решения поставленной задачи было выбрано семейство программных продуктов Rapid Miner (http://rapidminer.com/). Данная программа распространяется бесплатно и используется аналитиками и исследователями во всем мире для широкого круга задач, в частности для медицинских исследований. Отличительной особенностью рассматриваемого ПО является сочетание эффективности реализуемых в нем методов с дружественным интерфейсом, что делает эту программу легкодоступной для освоения непрограммирующими пользователями. Приложениями RapidMiner-а могут быть как исследовательские (модельные), так и прикладные (реальные) задачи интеллектуального анализа данных, включая анализ текста, анализ мультимедиа, анализ потоков данных. Еще одной важной особенностью этой программы является интегрирование данных из БД (из MS Access и MS Excel) в саму программу Rapid Miner.[2]

Разведочный анализ. На первом этапе исследования проводился предварительный анализ данных с целью выявления наиболее общих закономерностей, тенденций, характеристик и свойств анализируемых данных, законов распределения анализируемых величин. По каждому параметру были получены характеристики распределения и получены параметры описательной статистики, также были построены корреляционные матрицы и обнаружены параметры, связь между которыми наиболее сильна. После интеграции данных из Exel в среду Rapid Miner, программа проводит автоматический анализ загруженных данных и показывает таблицу со средними величинами данных и другими характеристиками. На рисунке 1 данные представлены в виде графиков, гистограмм и других визуальных инструментов.

Рис. 1. Представление данных в среде Rapid Miner

Кластеризация данных. На втором этапе исследования для определения групп пациентов, схожих по признакам, была решена задача кластеризации. Для создания предсказательной модели для каждой из групп пациентов будут рассчитаны свои коэффициенты уравнения регрессии. Для кластеризации данных был использован алгоритм k-means (k-means, fuzzy c-means, Густафсон-Кесселя). Действие алгоритма таково, что он стремится минимизировать суммарное квадратичное отклонение точек кластеров от центров этих кластеров. Алгоритм разбивает множество элементов векторного пространства на заранее известное число кластеров k. В качестве меры близости использовалось евклидово расстояние, вычисляемое по формуле:

$$D(x,y) = \sqrt{\sum_i (x_i - y_i)^2}\ . \qquad (1)$$

В этой группе популярны алгоритмы семейства k-средних, которые в качестве целевой функции используют сумму квадратов взвешенных отклонений координат объектов от центров искомых кластеров. Кластеры ищутся сферической либо эллипсоидной формы. В канонической реализации минимизация функции производится на основе метода множителей Лагранжа и позволяет найти только ближайший локальный минимум. [5] Использование методов глобального поиска (генетические алгоритмы) значительно увеличит вычислительную сложность алгоритма. Кластеризация полезна при определении различной информации, потому что она коррелируется с другими примерами, так что можно увидеть, где подобия и диапазоны согласуются между собой. Визуальный пример кластеризации изображен на рисунке 2.

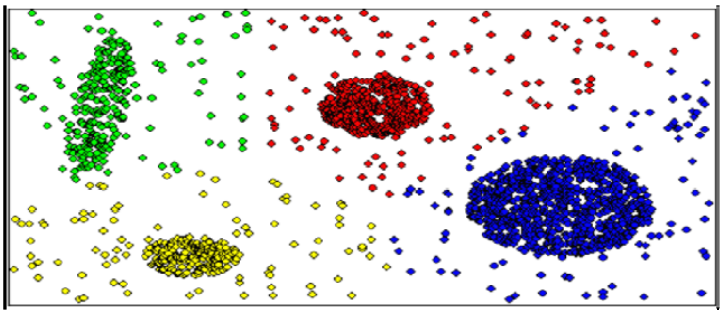


Рис. 2. Кластеризации алгоритмом k-means

В результате данные с помощью операторов кластеризации были разбиты по возрасту на шесть групп. Разбивать на кластеры пациентов будем с помощью упомянутого выше оператора K-means изображенным на рисунке 3.

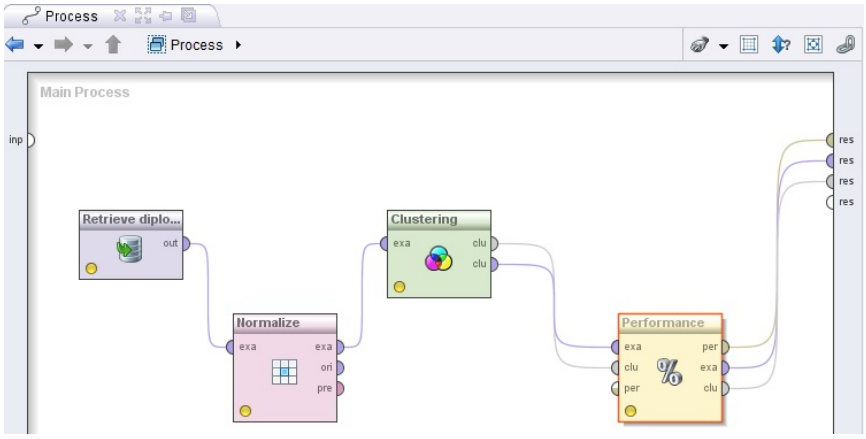


Рис. 3. Процедура кластеризации в программе Rapid Miner

Формирование предсказательной модели. Далее проводился регрессионный анализ полученных данных с целью создания модели зависимости целевых показателей от измеренных параметров. Формирование предсказательной модели происходило в два этапа.

Этап обучения. По известным независимым переменным (параметрам обследования $(X_1, X_2 ...)$ и известным зависимым переменным Y (сроки терапии) найдем коэффициенты для уравнения регрессии для каждой группы. Формула уравнения регрессии (формула 2) для расчета общего коэффициента который будет предсказывать срок заживления:

$$Y = A_1X_1 + A_2X_2 + A_3X_3 + \cdots + A_nX_n, \quad (2)$$

где, $X_1,...,X_n$ – параметр объекта;

$A_1,...,A_n$ – коэффициенты регрессии.

На этапе распознавания (если будут вводиться новые пациенты с неизвестным сроком заживления Y) по известным коэффициентам $A_1,...,A_n$, был найден срок терапии Y. Матрица регрессионной модели представлена на рисунке 4.

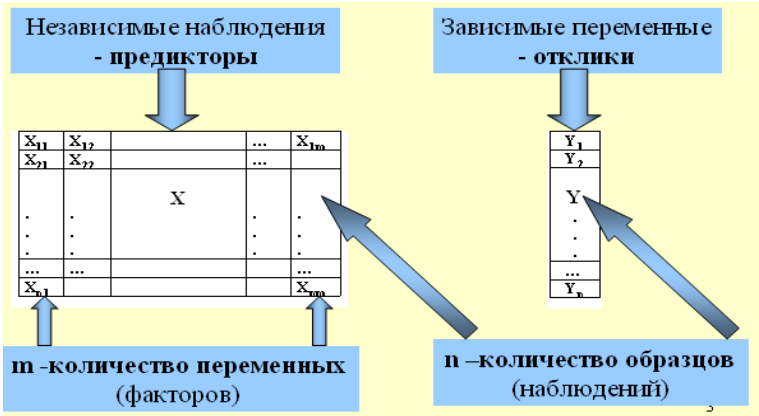


Рис. 4. Матрица регрессионной модели

Суть применяемого метода состоит в декомпозиции матрицы данных, определения зависимости между вектором признаков и матрицей исходных данных, формировании алгоритма зависимости – конструирования калибровочной модели и использования алгоритма для определения значений целевых показателей по новым данным. Для конструирования калибровочной регрессионной модели данные были разделены на два набора – обучающий, который использовался для идентификации модели, и проверочный – для проверки модели. Построенная модель применялась к данным из проверочного набора, и полученные результаты сравнивались с проверочными значениями. Таким образом, принималось решение о правильности, точности моделирования методом тест-валидации. Результаты проверки качества модели представлены на рисунке 5.

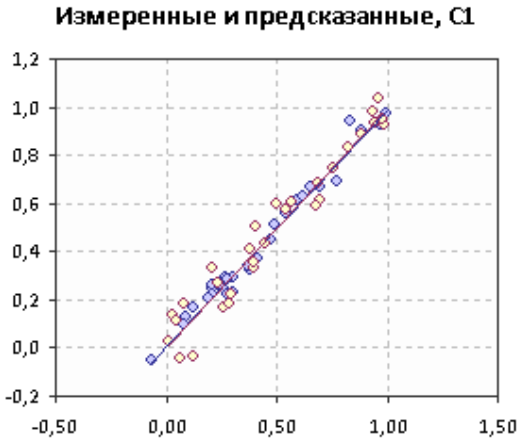


Рис. 5. Проверка калибровочной модели

В заключение можно сказать, что проделанная работа показала высокую эффективность внедрения новых технологий анализа данных в медицинские науки. Все проведённые исследования имеют практическую направленность, полученные результаты используются для повышения качества диагностики и ретроспективного анализа результатов обследования пациентов.

СПИСОК ЛИТЕРАТУРЫ

1. Барсегян А.А. и др. Методы и модели анализа данных: OLAP и Data Mining // А.А. Барсегян. – СПб., 2004, 88с.
2. Н. Паклин. Алгоритмы кластеризации на службе Data Mining. URL: http://www.basegroup.ru/library/analysis/clusterization/datamining /Дата обращения: 10.05.14.
3. Делакова Е.А. Создание алгоритма для обработки результатов медико-биологических исследований с помощью информационных технологий // Актуальные проблемы экономики современной России, Вып. 8. – СПб: ГУАП, 2012, С.36–39.
4. Делакова Е.А. Интеллектуальный анализ результатов медико-биологических исследований // Шестьдесят пятая научно-техническая конференция ГУАП.
5. В. Дюк, Data Mining – Учебный курс / В. Дюк, А. Самойленко. – М., 2001, С.14–44.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

УДК 004.9; 332.14:551.5

ОЦЕНИВАНИЕ РАЗВИТИЯ ОДНОГО КЛАССА СЛОЖНЫХ СИСТЕМ С УЧЁТОМ ПРИРОДНО-КЛИМАТИЧЕСКИХ ФАКТОРОВ

Ходаков Виктор Егорович[1], Соколова Надежда Андреевна[1], Антипенко Инна Владимировна[2], Бабина Ольга Витальевна[2],
[1] Херсонский национальный технический университет,
Россия, Крым, Херсон, Бериславское шоссе, 24,
[2] Керченский государственный морской технологический университет,
Россия, Крым, Керчь, ул. Орджоникидзе, 82,
e-mails: hodakov.victor@gmail.com, sergiiblack@gmail.com

Аннотация: В статье 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. 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. Представлены математические модели оценки состояния системы отклика в структуре развития региона. Сформированы критерии определения пространства состояний и разработка методов идентификации модели СЭС.

Ключевые слова: *система, многофакторный анализ, природно-климатические условия, регион.*

EVALUATION OF THE DEVELOPMENT OF CLASS COMPLEX SYSTEMS IN VIEW OF CLIMATIC FACTORS

Hodakov V.E., Sokolova N.A., Antypenko I.V., Babina O.V.,
e-mails: hodakov.victor@gmail.com, sergiiblack@gmail.com

Abstract: The methodology of multifactor estimation of a class of social-ecological systems – regions in view of the climatic conditions to select the economically active areas where production is characterized by minimum values of costs. To assess the state of SES used generalized functional design criteria ranked series. The methodology of multifactor estimation of a class of social-ecological systems - regions, taking into account the climatic conditions to select the economically active areas where production is characterized by minimum values of costs.Mathematical models assessing the state of the system response in the structure of the region. Formed the criteria for determining the state space and the development of methods to identify the model of SES.

Keywords: *system, multivariate analysis, climatic conditions, region.*

Введение. 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.

Все локальные (более элементарные) СЭС – это страны, регионы, территории, районы и их составные части – компоненты, такие как сложные территориально – распределённые объекты промышленной, коммунальной, энегретической среды и т.д. Эти СЭС в основном состоят из трёх групп главных элементов систем: социальных групп, экономических процессов и окружающей среды. Под окружающей средой (ОС) понимается экологическая, географическая, природно-климатическая среда и метасистемное окружение. Конкретные количественные и качественные характеристики перечисленных элементов и отношения между ними определяют конкретные свойства конкретной локальной СЭС.

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.

Человечество всегда для своего жительства выбирало территории с наиболее благоприятным для жизнедеятельности условиями (средами). В таких территориях производство характеризуется минимальными издержками и большей эффективностью. Это, так называемые, территории ускоренного экономического роста. Эта особенность человеческого бытия особенно проявилась на примере северных стран (Норвегия, Швеция, Канада и т.д.). Например, подавляющее большинство населения Норвегии (до 98%) проживает на узких морских побережьях, где особенно сильно чувствуется влияние тёплого течения Гольфстрим. Там же сформирован и основной промышленный потенциал страны.

Определение (выделение) внутри территорий стран зон, в которых производство характеризуется минимальными значениями издержек, требует разработки методологии оценивания зон (регионов), например, методологии оценивания устойчивости развития, инвестиционной привлекательности регионов (территорий) для выбора и развития экономически активных зон-территорий ускоренного развития.

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 [1].

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 [2], [3].

Рассмотрим формальные аспекты оценивания множества состояний СЭС

$$A\{0/a,\{A_a\}\supseteq\{A(0)\},a\},a\in A\,. \qquad (1)$$

Состояние объекта (СЭС) может быть представлено в виде отношений

$$R(X,Y,Z)\subseteq X\times Y\times Z\neq 0\,.$$

При функционировании объекта, взаимодействии объектов реализуется сложное пространственно-распределенное взаимодействие динамических объектов

$$\{P_{zj}\},\, j=J\,,$$

где J – множество индексов процессов, которые могут иметь детерминированный характер Д, стохастический, нечеткий $\widetilde{\mathrm{F}}$. При оценивании объектов $A(0)_a$ необходимо учитывать влияние на них множества факторов $\{\Phi_к\}$ и динамических процессов $\{P_{zj}\}$.

Необходимо определять состояние объекта $A(0)_a$ в координатах R (X,Y,Z) с учетом множества критериев, факторов $\{\Phi_к\}$ и динамических процессов $\{P_{zj}\}$.

В качестве обобщенного критерия оценки могут использоваться: уровень устойчивости развития региона, инвестиционная привлекательность, дискомфортность и др. Определение обобщенного критерия ориентирует на соответствующий отбор оцениваемых позиций и показателей, их характеризующих [2], [4].

Характеристика состояния объекта-региона определяется набором индикаторов (нормированных показателей – душевых, удельных и пр.). Оптимальный перечень индикаторов (показателей) должен соответствовать следующему:

– содержать не бесконечное, а ограниченное количество индикаторов (показателей);
– отражать все основные состояния и свойства социально-экономической системы;

– быть репрезентативным – способным отражать их полно и адекватно, в том числе в пространстве (учет объективных условий регионов) и во времени (фиксация не только моментного среза с использованием статических индикаторов, но и динамики ситуации с помощью индексов);

– быть методически корректным – со значениями индикаторов, упорядоченными по одному вектору (например, «чем больше – тем лучше», но с учетом смысла индикаторов, например, по безработице, бедности, преступности и т.п.);

– быть структурно выдержанным – без сильных диспропорций в количестве и качестве индикаторов по выбранным позициям, что может быть достигнуто с помощью агрегирования (формирования составных индикаторов).

Действующая система показателей, методология их сбора и обработки мало приспособлены для регионального уровня. Применяемые методы наблюдения, досчеты и дорасчеты, корректирующие коэффициенты не дают полной и объективной оценки происходящих в реальном секторе экономики процессов и явлений на уровне региона.

Всё это множество факторов, показателей являются частными показателями. Текущее состояние любой СЭС оценивается, как правило, достаточно большим количеством частных показателей $\{x_i\}=1$, каждый из которых отражает одну из сторон (сущностей) рассматриваемой системы. Это и есть многофакторное оценивание. Большая размерность набора показателей является существенным препятствием для изучения динамики такой системы, сравнения между собой отдельных систем и выработки оптимальных решений управления. Поэтому, естественным шагом в изучении таких систем является понижение их размерности, например, путем поступательной свертки частных показателей. Это не что иное, как переход к интегральной оценке объектов-регионов. В простейшем случае это замена определенного набора параметров $\{x_i\}_{i=1}^n$ единым более обобщенным показателем $I\left(\{x_i\}_{i=1}^n\right)$. Этот показатель принято называть индексом системы показателей $\{x_i\}_{i=1}^n$. При таком подходе к понижению размерности необходимо исключить потери информации о рассматриваемой системе и поэтому в основе построения всякого индекса лежит некая «разумная» процедура усреднений, например, вычисление среднего арифметического, среднего квадратичного, среднего геометрического и т.п.

Переход к более обобщенной интегральной оценке позволяет комплексно рассмотреть состояние системы, выявить положительные и отрицательные стороны её развития, провести сравнительный межрегиональный анализ. Всякий набор параметров $X=\{x_i\}_{i=1}^n$ можно трактовать как вектор в n-мерном евклидовом пространстве. Тогда всякий индекс $I\left(\{x_i\}_{i=1}^n\right)$ есть функционал на линейном пространстве размерности n:

$$I\left(\{x_i\}_{i=1}^n\right)=I(X), I:R_n\to R_1 .$$

Следующий употребительный класс индексов строится на основе квадратичных процедур усреднения (квадратичных функционалов): вычисления среднего квадратичного (эвклидовой нормы вектора)

$$J(X)=\sqrt{\frac{1}{n}\sum_{i-1}^{n}x_i^2}=\frac{1}{\sqrt{n}}\|X\| ,$$

либо вычисления среднеквадратического отношения вектора X от некоторого заданного оптимального вектора $S=\{S_i\}_{i=1}^n$

$$D(X)=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i-s_i)^2}=\frac{1}{\sqrt{n}}\|X-S\| .$$

В литературе нашли своё отражение несколько подходов к построению интегральных показателей, различающихся как по методам построения единого показателя, так и относительно выбора составляющих - системы показателей [2], [4].

В то же время в публикациях, посвященных структуре и вычислительным аспектам индексов СЭС какие-либо убедительные обоснования выбора той или иной процедуры усреднения при вычислении индексов, как правило, отсутствуют. Известные обоснования выбора конкретной процедуры усреднения проводятся либо на уровне «правдоподобных рассуждений», либо на уровне «здравого смысла». Анализ показывает, что наиболее употребительные процедуры усреднения и порожденные ими индексы имеют простую геометрическую интерпретацию и связаны между собой квадратичной зависимостью.

Не умаляя общности, можно полагать, что все допустимые состояния $X=\{x_i\}_{i=1}^n$ системы данного класса расположены в кубе

$$K=X=\{x_i\}_{i=1}^n\in R:0\le x_i\le 1, i=1,2,..n .$$

Этого всегда можно достичь соответствующей нормировкой допустимых параметров $\{x_i\}_{i=1}^{n}$.

Состояние СЭС характеризуется набором показателей, критериев, вся совокупность критериев каждого варианта может быть разбита на отдельные группы. Известно применение при оценке развития СЭС совокупность показателей разбивать на три группы показателей, а при оценке инвестиционной привлекательности на девять групп. Это справедливо только для тех случаев, когда не учитываются ПКФ. При учете ПКФ добавляется еще одна группа показателей, характеризующих природно-климатические факторы объекта [5], [6].

При анализе развития СЭС обобщенная оценка состояния учитывает параметры трех групп критериев:

$$I_{ИНВ} = Q_1\left(I_{ЭКИ}, I_{ЭН}, I_{СН}\right),$$

где $I_{ЭКИ}, I_{ЭН}, I_{СН}$ – критерии, определяющие характеристики соответственно экономического, экологического и социального направлений развития.

А при анализе инвестиционной привлекательности обобщенная оценка учитывает показатели следующих групп критериев:

$$I_{ИНВ} = Q_2\left(I_{ЭГП}, I_{РСП}, I_{ТП}, I_{ЭП}, I_{ИНФ}, I_{НТП}, I_З, I_{ИП}, I_{ИР}\right),$$

где $I_{ЭГП}, I_{РСП}, I_{ТП}, I_{ЭП}, I_{ИНФ}, I_{НТП}, I_З, I_{ИП}, I_{ИР}$, – критерии, определяющие соответственно характеристики экономико-географического положения, природно-ресурсного потенциала, трудового потенциала, экономического потенциала, емкости потребительского рынка, инфраструктурного, научно-технического потенциала, инвестиционных преференций, инвестиционных рисков СЭС.

Ключевой проблемой оптимального управления является использование адекватной математической модели объекта. Для получения математических моделей объектов СЭС и её компонентов используется идеология интроспективного анализа на основе экспертных оценок [7], [8], [9].

В силу особенностей СЭС получить строгую математическую модель поведения такого объекта не представляется возможным. Используются несколько подходов решения данной задачи.

В одном из наиболее распространенном подходе предлагается для оценки состояния СЭС использовать функционал обобщенного критерия, который получают на основе процедуры построения ранжированного ряда с использованием указанных выше критериев. Ранжирование – это процедура упорядочения, разбиения множества объектов в порядке предпочтения, с введением между ними некоторого порядка «лучше–хуже» [7], [8]. На основе своих знаний и опыта эксперт располагает объекты в порядке предпочтения, руководствуясь одним или несколькими показателями сравнения. В зависимости от вида отношений между объектами возможны различные варианты упорядочения.

Пусть среди объектов нет одинаковых по сравниваемым показателям, т.е. нет эквивалентных объектов. В этом случае между объектами существует только отношение строгого порядка, обладающее свойствами несимметричности (если $O_i \succ O_j$, то $O_j =\prec O_i$), транзитивности (если $O_i \succ O_j$, $O_j \succ O_k$ то $O_i \succ O_k$) и связности (для любых двух объектов либо $O_i \succ O_j$, либо $O_j \succ O_i$).

Из свойства связности вытекает совершенная (линейная) упорядоченность объектов. В результате сравнения всех объектов по отношению строгого порядка эксперт составляет упорядоченную последовательность

$$O_1 \succ O_2 \succ \ldots \succ O_n, \tag{2}$$

где объект с первым номером – наиболее предпочтительный из всех, объект со вторым номером менее предпочтителен, но предпочтительнее всех остальных и т.д.

В результате ранжирования при наличии отношений порядка и эквивалентности эксперт составляет упорядоченную последовательность, в которой некоторые объекты могут быть эквивалентными. Например, упорядочение может иметь вид:

$$O_1 \succ O_2 \succ O_3 \square O_4 \square O_5 \succ \ldots \succ O_{n-1} \square O_n.$$

В этой последовательности объекты O_3, O_4, O_5 эквивалентны между собой, а объекты $O_{n-1} \square O_n$ – между собой.

Ранжирование всегда производится в шкале порядков, независимо от того, имеются среди объектов эквивалентные или нет.

В практике ранжирования объектов, между которыми допускаются отношения как строгого порядка, так и эквивалентности, числовое представление выбирается следующим образом. Наиболее предпочтительному объекту присваивается ранг, равный единице, второму – второй ранг и т.д. Для эквивалентных объектов удобно назначать одинаковые ранги, равные среднему арифметическому значению рангов, присваиваемых одинаковым объектам. Такие ранги называют связанными.

Удобство использования связанных рангов заключается в том, что сумма рангов объектов равна сумме натуральных чисел от единицы до n. При этом любые комбинации связанных рангов не изменяют эту сумму. Это обстоятельство существенно упрощает обработку результатов

ранжирования при групповой экспертной оценке.

При групповой экспертной оценке каждый i-й эксперт присваивает каждому объекту j ранг r_{ij}. В результате проведения экспертного оценивания получается матрица рангов $\|r_{ij}\|$ размерности $n \times m$, где n – число объектов (j=1,…,n); m – число экспертов (i=1,…,m).

Ранги объектов определяют только порядок их расположения по показателям сравнения. Ранги как числа не дают возможности сделать вывод о том, на сколько или во сколько предпочтительнее один объект другого. Если, например, ранг объекта равен единице, то не следует делать вывод, что этот объект в три раза предпочтительнее объекта, имеющего ранг равный трем.

Достоинством ранжирования, как метода измерения, является простота осуществления процедур, недостатком – практическая невозможность упорядочения большого числа объектов. Как показывает опыт, при числе объектов больше 15–20 эксперты затрудняются в построении ранжированного ряда. Это объясняется тем, что в процессе ранжирования эксперт должен установить взаимосвязь между всеми объектами, рассматривая их как единую совокупность. При увеличении числа объектов количество связей между ними растет. Удержание и анализ большой совокупности взаимосвязей между объектами ограничивается психологическими возможностями людей. Поэтому при ранжировании большого числа объектов эксперты могут допускать ошибки.

Задача выбора наилучшего варианта оценки состояния СЭС методом ранжирования решается путем последовательной реализации следующих шагов:

– формирование вариантов реализации стратегий оценки состояний;
– выбор показателей и метрики оценок вариантов;
– формирование локальных критериев оценивания вариантов;
– формирование обобщенного критерия оценки;
– ранжирование вариантов по обобщенному критерию;
– выбор предпочтительного варианта (или множества наилучших).

В рамках решения указанных задач основным этапом принятия решения является возможность произвести оценку вариантов состояний и на этой основе установить порядок отношений (ранжирование).

Методологической основой решения данных задач является общая теория полезности. Если два решения $x_1, x_2 \in X$ соотносятся между собой как $x_1 > x_2$, то их функции полезности соотносятся как $P(x_1) > P(x_2)$.

Вид функции полезности принятого решения зависит от состава частных критериев вариантов для $I_{ур}$ или $I_{инв}$ и множества коэффициентов значимости этих критериев для лица, принимающего решения (ЛПР). Функцию полезности можно определить следующим образом:

$$P(x) = Q\left[a_i I_i(x)\right], i = \overline{1,n},$$

где a_i – коэффициент изоморфизма i-го частного критерия $I_i(x)$; Q – оператор преобразования.

При этом используются две формы представления функции полезности [10], [11], [12], [13], [14]:

– аддитивная

$$P(x) = \sum_{i=1}^{n} a_i I_i(x); \tag{4}$$

– мультипликативная

$$P(x) = \prod_{i=1}^{n} a_i I_i(x). \tag{5}$$

где a_i – весовые коэффициенты, $a_i \in [0,1]$, $\sum_{i=1}^{n} a_i = 1$.

Поскольку частные критерии имеют различную размерность и несравнимы между собой, они должны быть нормированы, то есть приведены к изоморфному виду. Тогда в функции полезности (4) или (5) используются нормированные значения частных критериев:

$$m\left[I_j(x)\right] = \frac{I_i(x) - I_{i-}}{I_{i-} + I_{i+}},$$

где $I_i(x), I_{i-}, I_{i+}$ – соответственно текущее, наихудшее и наилучшее значения частного критерия.

Аддитивная функция полезности будет иметь вид:

$$P(x) = \sum_{i=1}^{n} a_i m\left[I_i(x)\right].$$

В этом случае окончательный выбор варианта решения существенно зависит от величин коэффициентов значимости a_h, которые определяются экспертами. При этом форма представления

информации о значимости критериев может быть различной – детерминированной, вероятностной или в виде нечетких (лингвистических) переменных.

Распространенной ситуацией при оценке и выборе вариантов является задача, при которой эксперты не могут определить точные количественные значения весовых коэффициентов a_i, но способны предоставить качественную информацию относительно взаимной важности оцениваемых критериев:

$$I_1(x) \succ I_2(x) \succ \ldots \succ I_n(x).$$

В такой ситуации предлагается метод последовательного перебора критериев в порядке их важности.

Выводы. 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. 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.

СПИСОК ЛИТЕРАТУРЫ

1. Ходаков В.Е., Соколова Н.А., Чёрный С.Г. Влияние природно-климатических факторов на социально-экономические и производственные системы. Херсон: Из-во Гринь, 2013. С. 354.
2. Глушков В.М., Иванов В.В., Яценко В.М. Моделирование развивающихся систем. Монография. М.: Наука, 1983. 350с.
3. Кучеренко Е.І. Теоретичні основи та технології оцінки технічного стану просторово-розподілених об'єктів. Монографія. Київ: Техніка, 1991.
4. Згуровский М.З., Стасюха Г.А. Роль инженерной науки и практики в устойчивом развитии общества // Системні дослідження та інформаційні технології. 2007. № 1. С. 19–38.
5. Горбачева Ю.И. Инвестиционная привлекательность Украины и ее регионов // Коммунальное хозяйство городов. 2004. Вып.56. – С 58-65.
6. Петров Э.Г., Губаренко Е.В. Требования к системам комплексного мониторинга социально-экономических систем // Проблеми інформаційних технологій. 2011. № 1(09). С. 102-107.
7. Corruption Perceptions Index – 2012 – Режим доступа: http://cpi.transpagency.org. Заголовок с экрана.
8. Коваленко И.И., Драган С.В., Дыхальский М.А. Экспертные оценки в управлении инновационными проектами. Николаев: НУК, 2007. 168 с.
9. Интроспективный анализ. Методы и средства экспертного оценивания: монография / В.В. Крючковский и др. Херсон: Из-во Гринь Д.С., 2011. 168с.
10. Овезгельдиев А.О., Петров Э.Г., Петров К.Э. Синтез и идентификация моделей многофакторного оценивания и оптимизации. Киев: «Наукова думка», 2002. 164 с.
11. Черный С.Г. Клиент-серверное приложение в структуре выбора проектного решения с учетом нечеткого выбора целей. Материалы XXIX конференции памяти выдающегося конструктора гироскопических приборов Н.Н.Острякова Санкт-Птербург, 2014. С. 410-417.
12. Черный С.Г., Логунова Н.А. Разработка сегментов кластеров координации отраслевой направленности. Мир транспорта. 2014. Т. 12. № 3 (52). С. 104-115.
13. Черный С.Г. Анализ правил комбинирования групповых экспертных оценок при нечетких данных. Системы управления и информационные технологии. 2014. Т. 57. № 3.1. С. 182-187.
14. Жиленков А.А., Чёрный С.Г. Элементы структурной модели устройства аппроксимации для задач идентификации и контроля параметров объектов управления. Проблемы машиностроения. 2013. Т. 16. № 4. С. 62-65.

УДК 629.075

АНАЛИЗ ПРОБЛЕМ ИХТИОЦЕНОЗА МОРСКОЙ ЭКОСИСТЕМЫ НА ОСНОВЕ КОГНИТИВНОЙ ГРАФОВОЙ МОДЕЛИ

Михайлов Владимир Валентинович[1], Переварюха Андрей Юрьевич[1],
Соловьева Инна Владимировна[2]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия, 39,
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, Большая Морская ул., 67,
e-mails: mwwcari@mail.ru, madelf@pisem.net, inna.solovyeva@gmail.com

Аннотация: Проблемы при эксплуатации природных ресурсов и стремительное истощение рыбных запасов в условиях стремительного изменения среды требуют гибких подходов к предварительному анализу и являются сложным объектом для классического вычислительного моделирования. Статья посвящена применению метода концептуальной структуризации информации о взаимодействии природных и антропогенных факторов на основе когнитивных моделей. Формальный анализ импульсов в знаковом графе в контексте исследуемой ситуации деградации биоресурсов Каспийского моря способствовал разработке в рамках проекта РФФИ оригинальной гибридной динамической системы для моделирования эффективности воспроизводства осетровых рыб. Показано, как выбор математического подхода к описанию ситуации строится на результатах когнитивного анализа

экологических взаимосвязей. Интерпретация наблюдаемых изменений поведения моделей позволила выявить скрытый контур отрицательной обратной связи в искусственном воспроизводстве рыб.

Ключевые слова: *Компьютерное моделирование популяционных процессов, методы когнитивной структуризации, гибридные динамические системы, графовые модели в экологии*

ANALYSIS OF PROBLEMS OF ICHTHYOCENOSIS OF THE MARINE ECOSYSTEM BASED ON COGNITIVE GRAPH MODEL

[1]Mihaiylov Vladimir,[1]Perevaryukha Andrey,[2]Solovyeva Inna
[1]St.Petersburg Institute for Informatics and Automation of the RAS
[1]Russia, St. Petersburg 14 line, 39,
[2]St.Petersburg State University of Aerospace Instrumentation,
[2]Russia, St. Petersburg, Bolshaya Morskaia str. 67,
e-mails: mwwcari@mail.ru, madelf@pisem.net, inna.solovyeva@gmail.com

Abstract:Ecological processes in the face of rapid changes in the environment as an object for the computer simulation requires a flexible approach to the analysis. Article devoted to applications of the conceptual structuring of ideas about the interaction natural and anthropogenous factors on the basis of cognitive models. The formal analysis of pulses in the sign graph in the context of the situation degradation bioresources of Caspian Sea has promoted the development of original hybrid dynamic systems for modeling sturgeon fish reproduction. It is shown that the choice of the mathematical approach to the description of the situation can be based on the results of cognitive analysis of the ecological relationships. At the conclusion of results of computational studies should logically follow the newly theoretical interpretation of the observed changes in behavior of models.

Keywords: *Computer modeling of population processes, methods of cognitive structurization, hybrid dynamic systems, ecology graph models*

Для этапа анализа сведений о противоречивом влиянии различных факторов развиваются когнитивные методы системного анализа, работающие с качественной информацией. В статье рассматриваются методы когнитивной структуризации, которые могут стать «указующим перстом» в формировании динамических моделей экологических процессов, так и использоваться при сущностной интерпретации результатов вычислительных экспериментов.

Долгосрочная оценка многообразия последствий вмешательства является задачей междисциплинарных исследований. Наиболее существенно последствия зарегулирования стока рек отражаются на возможностях размножения анадромных видов, лососевых и осетровых. Для созревающих в море рыб становятся недоступными используемые ранее пригодные для нереста участки в верховьях рек. Восполнить потери в воспроизводстве популяций ценных промысловых рыб Волги предполагалось за счет технологии искусственного оплодотворения икры, искусственного выращивания молоди и последующего ее выпуска.

В 1975 г. была принята стратегия максимизации ежегодного вылова (до 30 тыс. т.) за счет выпуска (порядка 90 млн. шт.) молоди осетровых как основного источника формирования запасов, способного не только компенсировать, но и превзойти потери в естественном воспроизводстве при гидростроительстве. В результате строительства рыбоводных предприятий для искусственного выращивания молоди к поставленной цели резкого увеличения масштабов выпуска удалось приблизиться. В 1977 г. уловы осетровых достигли своего максимума – 27,3 тыс. т., однако затем начали неуклонно уменьшаться. Ситуация с промыслом осетровых рыб Каспия развивалась в точном соответствии с предупреждением, высказанном в 1950 г. основоположником метода гормональных инъекций профессором Н.Л. Гербильским: «поддержать относительно благополучное в численном отношении стадо неизмеримо легче, чем восстанавливать его из жалких остатков». На настоящий момент эксперты Международного союза охраны природы (IUCN) констатируют деградацию трех популяций осетровых Каспия, имеющих с 2010 г. в Красной книге статус «Critically Endangered». Ихтиологами неоднократно проводилась переоценка реальной величины промыслового возврата от искусственного воспроизводства, и получение достоверной оценки представляет существенную сложность. Подтверждено, что изначально заложенный в планах 1970-х гг. коэффициент промыслового возврата заводской молоди в размере 3% оказался завышенным. В 1989 г. определялись для осетра 1,2%, севрюги 1%, белуги 0,1%. В 1998 г. для осетра 0,7% , севрюги 0,83%, белуги 0,07%. Оценка динамики снижения реальной выживаемости на ранних этапах жизненного цикла рыб важна при планировании мер по сохранению генофонда деградировавших популяций. Отдельную задачу представляет анализ причин невыполнения прогнозов 70х гг. в сопоставлении с динамикой экосистемных изменений на фоне которых был организован рыбоводный процесс и определялась величина допустимого вылова.

Гидростроительство повлекло перемены в трофической цепи ихтиоценоза Нижней Волги, изменив соотношения доминирования автохтонных рыб и поспособствовав расселению

растительноядных видов вселенцев. По естественным причинам менялась гидрологическая обстановка региона. Период регрессии сменился в 1978 г. быстрым и неожиданным для климатологов повышением уровня Каспия. Для бессточного озера площадью более 370 тыс. км.^{2} исторически характерны колебания уровня, которые сложно предсказывать. Амплитуда за период наблюдений составляет 3,8 м. Подъем моря рассматривался экспертами как благоприятный фактор, так как прогнозировалось увеличение площади акваторий Северного Каспия. В прогнозах не брались в расчет ряд значимых факторов. Так на фоне деградации осетровых уловы их пищевых конкурентов аналогично уменьшались, что не укладывается в выводы из вольтерровской модели, описывающей динамику конкурирующих за один ресурс двух ограниченных популяций.

Очевидно, что эволюционно сложившаяся стратегия размножения осетровых рыб, выразившаяся в существовании нескольких сезонных рас и длинных миграционных путях, позволяли поддерживать высокую биомассу рыб при относительно небольшой кормовой биомассе. Соответственно, актуально создание компьютерной модели формирования пополнения популяций, позволившей анализировать сценарии несоответствия развития рыбного хозяйства с эволюционным трендом анадромных рыб Каспия. Вмешательство в естественный репродуктивный процесс запустило подобно падающим костяшкам домино неизвестный ранее экспертам комплекс обратных связей в механизмах экологической регуляции. Вселение видов различных фаунистических комплексов, нестабильность речного стока, смена периодов регрессии и трансгрессии моря во взаимосвязи с антропогенными факторами привели к непрогнозируемому развитию ситуации. Анализ возможных причин несоответствия планировавшейся эффективности искусственного воспроизводства и прогнозируемой величины промыслового возврата является актуальной задачей для исследований с применением компьютерного моделирования сценариев развития противоречивой ситуации.

Формальное исследование процессов в больших экосистемах относится к области системного анализа слабоформализованных проблем. Перспективным подходом для получения формального представления взаимосвязи факторов являются методы когнитивной структуризации разнородной информации, например использованные в для информационного обеспечения при построении проблемно ориентированных биомедицинских баз знаний. Взаимовлияние между конечным множеством факторов целесообразно исследовать на уровне описания качественных изменений, так как они отражаются в литературе специалистами в сравнительно-оценочных формулировках, как например «благоприятность условий нагула рыб». Одним из подходов к гибкому трансформированию знаний в структуры данных в слабоформализованных областях служат методы построения и анализа когнитивных орграфов в специализированных информационных средах.

Когнитивный орграф будем рассматривать в первую очередь как инструмент для формирования наиболее полноценных гипотез о функционировании популяционного процесса при определенных внешних воздействиях. Применение концептуальной структуризации может изменить сложившиеся стереотипы, которыми оперируют в предметной области и способствовать развитию модифицированных математических подходов к прогнозированию риска истощения эксплуатируемых биоресурсов.Когнитивный подход предполагает формализацию гипотезы о функционировании системы в виде знакового орграфа, вершинам которого сопоставляются выделенное множество факторов, а ребрам знаки «−» и «+». Ребрам можно сопоставить веса, если будет определена универсальная шкала взаимодействий для всей рассматриваемой проблемы.

Развиваются модификации методологии применения когнитивных графов, позволяющих на качественном уровне формализовать ситуацию в виде множества концептов и направлений передачи воздействия по различным путям. Формализм взвешенных знаковых графов является расширением представления орграфа *G*(X, E), которое дополняется множеством параметров вершин V, где каждой вершине x_i ставится в соответствие параметр-концепт $v_i \in V$ и функционалом преобразования дуг *F*(V, E), который определяет в соответствие дуге орграфа знак (или вес).

Функционал преобразования определяется следующим образом:

$$F(v_i, v_j, e_{ij}) = \begin{cases} +u_{ij}, \text{ если при увеличении } v_i \text{ увеличивается } v_j; \\ -u_{ij}, \text{если при увеличении } v_i \text{ уменьшается } v_j. \end{cases}$$

где u_{ij} может принимать значения из конечного множества B, при рассмотрении только знака влияния $\mathrm{B} = \{-1, 1\}$.

В популярной монографии Ф. Роберстс последовательные изменения значений параметров соответствующих вершинам предлагал рассматривать как импульсные процессы в дискретном времени [11].

Импульс в вершине определим как изменение значения ее параметра v_j в момент n:

$$p_j(n) = v_j(n) - v_j(n-1) \text{ при } n > 0.$$

В импульсном процессе значение параметра вершины будет изменяться:

$$v_i(n+1) = v_i(n) + \sum_{\substack{j=1 \\ j \neq i}}^{N} F(v_i, v_j, e_{ij}) p_j(n). \quad (1)$$

Наиболее интересные выводы можно получить, рассматривая импульсные процессы вида (1) в графах с замкнутыми путями. Проведем структуризацию обобщенных нами из различных и часто противоречивых источников сведений о характере и степени выраженности взаимодействия факторов, влияющих на благополучие волжских популяций осетровых рыб в виде знакового когнитивного орграфа. Ретроспективный анализ промысловой статистики и разнообразных экспертных мнений позволил выделить основные факторы, пригодные для когнитивной структуризации. Суждения специалистов часто противоречивы, но компьютерная среда может реализовать набор сравнительных сценариев. Программная реализация взвешенного орграфа строится на основе стандартных средств объектно-ориентированного программирования.

В качестве концептов, определяющих процессы в экосистеме и влияющих на динамику запасов осетровых рыб, выделим следующие 12 природных и антропогенных факторов и поставим в соответствие вершинам нашего когнитивного орграфа *G*(X,E,V):

v_1 – численность нерестового стада осетровых рыб; v_2 – численность пополнения; v_3 – естественная (компенсационная) смертность; v_4 – благоприятность условий нагула осетровых; v_5 – эффективность естественного воспроизводства; v_6 – масштабы искусственного воспроизводства; v_7 – уровень промысловой эксплуатации нерестовой части популяции; v_8 – биомасса доминирующего вида моллюсков; v_9 – плотность кладок икры на нерестилище; v_{10} – изменение уровня Каспийского моря; v_{11} – степень загрязнения Нижней Волги; v_{12} – протяженностей доступных путей анадромной миграции.

В результате сопоставления данных наблюдений, анализе литературы об историческом развитии экосистемы и формализации ряда экспертных мнений удалось сформировать когнитивный орграф, включающий соответствующих концептам 12 вершин и множество взвешенных дуг, отражающих знак и степень взаимовлияния (рисунок 1)

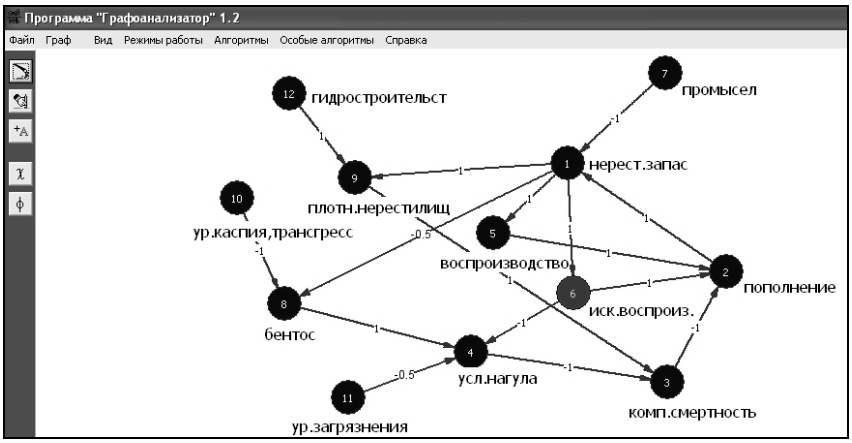


Рис. 1. Когнитивный орграф взаимовлияний в экосистеме Каспия

Очевидно, что представленное дугами качественное влияния разнится по своей выраженности, потому подобно физикам разумно охарактеризовать в экологии условно «сильное» и «слабое» взаимодействие. Негативное действие промысла и загрязнения на биоресурсы различны, потому последнее влияние определенно как «слабое» с $u = -0.5$. Импульсные процессы для графа рис. 1 целесообразно запускать из вершин v_6 и v_7 .

На основе оценки динамики значений v_4 , v_2 орграфа сформирована гипотеза, что темп роста молоди должен влиять на скорость убыли численности поколения и при этом должно существовать некоторое пороговое значение веса, после которого действие неблагоприятных факторов должно резко уменьшаться. Характер пульсации значения v_3, предсказывает, что темп роста в свою очередь должен зависеть от плотности скопления молоди и тогда может наблюдаться зависимость выживаемости от плотности с несколькими экстремумами, которая не описывается известными ранее моделями. Представим аналогичную модели Рикера зависимость в форме дифференциального уравнения для убыли численности $N(t)$, решаемого на определенном отрезке [0, *T*]:

$$\frac{dN}{dt} = -(\alpha N(0) + \beta)N(t),\ \ t \in [0,T]. \tag{2}$$

Константы в (2) соотносятся с параметрами Рикера: $a = \lambda \exp(-\beta T), b = \alpha T.$ λ – средняя плодовитость особей популяции, определяющая начальные условия $N(0) = \lambda S.$

Гипотеза в (2) о зависимости смертности от начальной численности $N(0)$ весьма специфична только для ситуации сильного каннибализма. Необходимо дополнить модифицированное (2) уравнением, отражающим среднее размерное развитие в условиях ограниченности доступных кормовых организмов. Учтем характерное обстоятельство, что уязвимость для хищников молоди резко уменьшается по мере роста, так взрослые осетровые не имеют естественных врагов. Скорость размерного развития представим в уравнении обратно зависящей от дробной степени плотности:

$$\frac{dw}{dt} = \frac{g}{\sqrt[k]{N(t)} + l}, k < 3, \tag{3}$$

где g – параметр объема доступных кормовых ресурсов, l – учитывает ограничение скорости развития не связанное с численностью поколения.

Длительность интервала уязвимости, того периода в жизни поколения, когда смертность зависит от плотности, может вычисляться в модели в зависимости от интенсивности роста поколения, что экологически обосновано. Положим, что при достижении некоторого $\hat{w}$ смертность обусловлена промысловыми причинами. Сформируем систему дифференциальных уравнений, описывающих динамику убыли численности поколения до вступления в нерестовую часть популяции $S = N(T), T = v(w)$:

$$\begin{cases} \dfrac{dN}{dt} = -(\alpha w(t)N(t) + \overline{f}(N(0))\beta)N(t) \\ \dfrac{dw}{dt} = \dfrac{g}{\sqrt[k]{N\ (t)} + l}, \quad k < 3, \qquad\qquad w < \hat{w} \end{cases}, \tag{4}$$

где α – мгновенный коэффициент компенсационной смертности; β – коэффициент не зависящей от плотности декомпенсационной смертности; начальные условия задаются: $w(0) = w_0,\ N(0) = \lambda S.$ Функция $\overline{f}$ должна обладать свойством $\overline{f}(S) > 1, S < L$ и $\overline{f}(S) \to 1, S \square\ L$ отражающим факт резкого уменьшения эффективности воспроизводства при малой численности нерестового стада, меньшей некоторой критической L.

Модель формирования пополнения (4) рассматривается как непрерывно-дискретная динамическая система и алгоритмически реализуется в вычислительной среде *AnyLogic* в форме гибридного автомата с предикативным переходом. В некоторый выделяемый момент гибридного времени происходит переопределение начальных условий для расчета задачи Коши на следующем в последовательности кадре непрерывного времени. Поведение гибридной системы «склеивается» из непрерывного изменения состояния и дискретных событий, переопределяющих развитие процесса.

Множество решений задач Коши для допустимых $S \in \square^+$ определит интересующую нас зависимость $\varphi(S)$, называемую «кривой воспроизводства» популяции. График (4), полученный в вычислительной среде задает унимодальную кривую с ненулевой горизонтальной асимптотой и двумя нетривиальными пересечениями R_1^*, R_2^* с биссектрисой координатного угла *R*=*S*, геометрическим местом стационарных точек.

Полученная зависимость с пологой восходящей ветвью и ниспадающей правой с уменьшающимся наклоном позволил преодолеть два важных недостатка, отмеченных специалистами, применявшими функцию Рикера для практических задач.

Основной недостаток функции $f(x) = ax\mathbf{e}^{-bx}$ – наибольшее значение производной достигается при стремлении аргумента к нулю, но вряд ли наибольший прирост воспроизводства может достигаться при таких условиях:

$$f'(x) = a\mathbf{e}^{-bx}(1 - bx), \quad \lim_{x \to 0} a\mathbf{e}^{-bx}(1 - bx) = a.$$

Неудобное свойство $\lim_{x\to\infty} ax\mathbf{e}^{-bx} = 0$ не соответствует экспериментальным данным и устранялось обычно при моделировании простым переопределением в вычислительном алгоритме $f(x)$ в кусочно-заданную функцию с интервалом постоянного значения $f(x) = K, x > x_1$.

Качественное отличие разработанной непрерывно-дискретной динамической системы от ранее предлагавшихся дискретных моделей заключается в наличии двух областей притяжения аттракторов в фазовом пространстве Θ_1, Θ_2. Границей между областями служит неустойчивая стационарная точка первого пересечения с биссектрисой R_1^*, когда точка R_2^* устойчива до момента бифуркации удвоения. Аттрактором для области Θ_1 служит начало координат т.е. тривиальное равновесие. Следовательно, R_1^* есть критически допустимая численность для продолжительного существования популяции. Переход траектории модели в область Θ_1 интерпретируется как запуск процесса необратимой деградации популяции.

Системный анализ и последующие исследование вычислительными методами модели на основе системы дифференциальных уравнений (4) показывает, что для популяций анадромных рыб с длинным жизненным циклом неприменима популярная стратегия оптимального промысла, ставящая цель получения максимально допустимого стабильно вылова. Рискованный промысел может привести к началу процесса необратимой деградации популяций. Возместить потери в естественном воспроизводстве на фоне промыслового давления добившись только массового выпуска заводской молоди в русла рек нереалистично. Искусственное воспроизводство требует новых исследований жизненного цикла молоди, так сейчас базируется на результатах полученных при других экологических условиях.

Целесообразно отметить отдельные недостатки формализма когнитивных графов применительно к задаче системного анализа экологических проблем и динамики промысловых запасов. Факторы влияют друг на друга с различной скоростью. Для экологических процессов свойственно явление запаздывания во времени. Например, обеспеченность особей необходимыми ресурсами зависит не от текущей численности, а от плотности поколения на предыдущей стадии развития и в так случае в правой части уравнения необходимо использовать функционал с отклоняющимся аргументом: $\Psi\left[N(t-\tau)\right]$. Вероятным усовершенствованием представляется допустимость для модели подсистемы выделения подграфа $G_1(X_1, E_1, V_1)$ с функционалом преобразования дуг другой формы. Вполне вероятно в алгоритме обработки орграфа предусмотреть предикативное изменение знака дуги между концептами, так как «положительность» влияния тоже может быть относительной.

*Работа выполнена в рамках Проекта **РФФИ** № 15-07-01230* (рук. Михайлов В.В.).

СПИСОК ЛИТЕРАТУРЫ

1. Ходоревская Р.П., Рубан Г.И., Павлов Д.С. Поведение, миграции, распределение и запасы осетровых рыб Волго-Каспийского бассейна.– М.: Тов-во науч. изд. КМК, 2007. 242 с.
2. Ризниченко Г.Ю. Математические модели в биофизике и экологии.– Ижевск, 2003. 183 с.
3. Карпинский М.Г. Экология бентоса Среднего и Южного Каспия.– М.: Изд. ВНИРО, 2002. 283 с.
4. Авдеева З.К., Коврига С.В., Макаренко Д.И., Максимов В.И. Когнитивный подход в управлении // Проблемы управления, 2007. №3. С. 2–8.
5. Кульба В.В., Миронов П.Б., Назаретов В.М. Анализ устойчивости социально-экономических систем с использованием знаковых графов // Автоматика и телемеханика. 1993. №7. С.130–137.
6. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. М.: Наука, 1986. 496 с.
7. Ricker W. E. Stock and Recruitment // Journal of the Fisheries Research Board of Canada, 1954. Vol. 11. N.5. P. 559–623.
8. Feigenbaum M.J. Universal behavior in nonlinear systems // Physica D, 1983. Vol. 7. №1–3. P. 16-39.

УДК 532.22

ФЕНОМЕНОЛОГИЧЕСКАЯ МОДЕЛЬ ПОВТОРЯЮЩИХСЯ ВСПЫШЕК ЧИСЛЕННОСТИ ВРЕДИТЕЛЕЙ ЛЕСА

Переварюха Андрей Юрьевич[1], Мосейко Алексей Григорьевич[2],
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14-я линия, 39,
[2]Санкт-Петербург, Зоологический институт Российской академии наук,
Россия, Санкт-Петербург, Университетская набережная, 1,
e-mails: madelf@pisem.net, chrysolesha@mail.ru

Аннотация: обсуждается динамическая система, дискретная составляющая траектории которой отличается наличием переходного хаотического поведения. Непрерывно-событийная структура алгоритмически реализована в вычислительной среде на основе системы дифференциальных уравнений убыли поколений. Свойства имитируют продолжительные стохастические флуктуации, которые наблюдаются для ряда популяций вредителей леса. С дополнением правых частей уравнений специализированными функционалами сформирована феноменологическая модель, описывающая наличие критических уровней, особых для экосистемы соотношений параметров. Достижение состояний резко меняет развитие популяционного процесса, являясь механизмом запуска вспышки численности, когда популяция на повторяющихся промежутках существования оказывается вне действия регулирующих эффективность ее воспроизводства факторов.

Ключевые слова: *периодические вспышки популяций насекомых; повторяющиеся пороговые эффекты; нелинейность в биологических процессах; флуктуационные режимы.*

PHENOMENOLOGICAL MODEL OF REPETITIVE OUTBREAKS OF POPULATIONS OF THE FOREST PESTS

Perevaryukha Andrey[1], Moseyko Alexey[2],
[1]St.Petersburg Institute for Informatics and Automation of the RAS,
[1]Russia, St. Petersburg 14 line, 39,
[2]Zoological Institute of the Russian Academy of Sciences,
[2]Russia, St. Petersburg Universitetskaya emb, 1,
e-mails: madelf@pisem.net, chrysolesha@mail.ru

Abstract: We have developed a hybrid dynamical system, discrete component of the trajectory is characterized by the presence of transition chaotic behavior. Continuous-discrete structure is algorithmically implemented in a computing environment based on a system of differential equations for the velocity decrease of generations. The resulting properties can simulate prolonged stochastically caused fluctuations that occur for a number of populations Hemiptera pests. With the addition of right-hand sides of equations by the specialized trigger functionals is formed computational model that describes the availability of critical levels, special rare ecosystem relationships between the parameters. Achieving such states dramatically changes the development process of the population, as a mechanism for resetting the outbreak, when the population for a limited time interval of existence is outside the action of regulatory effectiveness of its reproduction factors.

Keywords: *occasional outbreaks of insect populations; repetitive threshold effects; nonlinearity in biological processes; fluctuational regimes.*

Рассматривается задача вычислительного моделирования вспышки численности насекомого, требующая достижения особых нетривиальных свойств фазового портрета для разрабатываемой динамической системы. Моделируемый процесс выражено разбивается на последовательность существенно отличающихся фаз, что предопределило оригинальность выбора математического аппарата на основе гибридного времени. Для переходов между фазами процесса использован метод контролируемой реализации качественных метаморфозов поведения динамической системы. Предложена дискретно-непрерывная вычислительная модель, описывающая эффект самопроизвольного перехода от апериодических флуктуаций к фазе взрывообразно ускоряющегося репродуктивного процесса с последующей фазой быстрого спонтанного затухания. Модель биологически обоснована на примере анализа данных о сценарии вспышки у полужесткокрылых видов насекомых, поражающих определенный вид растений.

В математической биологии предложено значительное число популяционных моделей, но явление вспышки численности остается проблемой для моделирования, во многом потому, что такая динамика нарушает эволюционно сложившиеся принципы функционирования природных процессов. Сценарий начала вспышки противоречит классическим непрерывным моделям лимитированных популяций, где динамика вида задается уравнением $f'(t) = f(N)$ с точкой $f''(\hat{N}) = 0$, и дальнейшим снижением скорости роста при $f''(N) < 0$ до его прекращения в точке $f'(N^*) = 0$. Наблюдения энтомологов обосновывают существование значения $\bar{N}_{\mathrm{I}}$, когда после достижения $N > \bar{N}_{\mathrm{I}}$ прирост численности наоборот резко увеличивается [1]. Пороговое значение не должно быть банально достижимо из любого другого состояния модели, иначе вспышки одного вида наблюдались бы чаще. Дополнительно модель должна позволять имитировать стохастические флуктуации, характерные для популяций вредителей, развитие которых подвержено действию случайных погодных факторов.

1. Формализация динамики последовательных поколений

Мы предлагаем реализовать в модели две основные идеи: дифференцированное описание силы действия факторов в разных состояниях популяции и наличие для модели неустойчивого равновесия в популяционном процессе, преодоление которого начинает фазу стремительного увеличения. Подходящими для явления вспышки представляется методов моделирования колебаний эффективности репродуктивного цикла и изменений факторов смертности на последовательных стадиях развития.

Представим, что интервал между репродуктивными циклами непрерывного времени имеет фиксированную длину $[0,T]$. Численность поколения можно описывать от некоторой начальной $N(0)$ генерации дифференциальным уравнением, вычисляя на краю промежутка число особей S, доживших до следующего момента размножения:

$$\frac{dN}{dt} = -(\alpha N(0) + \beta)N(t), \ \ t \in [0,T]. \tag{1}$$

Численное решение задачи Коши (1) с коэффициентами мгновенной смертности α и β задает куполообразную кривую зависимости восполнения поколений $S = \varphi(N(0)), N(0) \in Z^+$ с нулевой горизонтальной асимптотой и единственным нетривиальным пересечением с биссектрисой координатного угла S^*.

Сильная зависимость смертности от первоначальной численности для насекомых вредителей растений не характерна. Положим, что рост особей $w(t)$ в раннем онтогенезе лимитирован доступностью не возобновляемого ресурса q, замедляясь с увеличением числа его потребителей. Подобное предположение было использовано в модели пополнения для учета роста молоди рыб в [2] просто в виде обратной зависимости от текущей численности $w'(t) = f(N^{-1})$. Модифицированное уравнение условного развития опишем обратной дробно-степенной зависимостью и поправкой δ:

$$\frac{dw}{dt} = \frac{q}{\sqrt[3]{(N(\mathrm{t}) + \delta)^2}} \tag{2}$$

Правую часть (1) модифицируем с учетом увеличения потребления ресурса:

$$\frac{dN}{dt} = -\alpha w(t) N^2(t) - \beta N(t) \tag{3}$$

Объединяя в систему (2) (где показатель дробной степени в знаменателе можно рассматривать как параметр) и уравнение (3), можно в вычислительной среде получить кривую с одним максимумом и ненулевой асимптотой и применять модель, переопределяя начальные условия (2) на концах непрерывных промежутков: $N_{n+1}(0) = \lambda S_n, w(0) = const$, λ средняя плодовитость популяции. Таким методом получим дискретную траекторию, где роль оператора эволюции выполняет численное решение системы дифференциальных уравнений на промежутке времени [3].

Обоснованным развитием подхода мы представляем непрерывно-событийную структуру, где изменения происходят при достижении особых условий внутренних переменных системы. Реализовать предикативную структуру возможно с применением методов современной теории гибридных систем [4]. Их преимущества в том, что если представить сложную скачкообразную эволюцию процесса в виде графа с переходами, то гибридная система может рассматривать переходы не между состояниями, а между поведениями. Нужно описать особым образом в модели действие вносящих нелинейность экологических эффектов.

Повышение численности приводит к исчерпанию ресурсов, что обычно ведет к плавному замедлению темпа роста популяции и стабилизации, но для вредителей леса более правдоподобна фаза стремительного снижения численности. Репродуктивный процесс при низкой численности аналогично имеет свои нелинейные особенности. Любой инвазионный процесс вида в новой среду проходил этап «бутылочного горлышка» существования малой группы особей, перед тем как продемонстрировать стремительное увеличение [5]. Не все виды преодолевают этап бутылочного горлышка.

В популяционной экологии широко обсуждается по данным различных наблюдений действие «эффекта агрегированной группы» [6]. Замечено повышение выживаемость молоди в группе особей при том, что такая скученность увеличивает пищевую конкуренцию взрослых. Соответственно, в малочисленных группах эффективность воспроизводства будет непропорционально снижаться и специалистами дискутируется наличие для популяций разных видов наличие критически низкого значения. Многим вредителям для преодоления химической защиты растений требуется массовость, потому неоднократно проникавший в Новый Свет с первыми кораблями европейцев короед *Ips typographus* не закрепился в американских лесах. Исследования в работе [7] на примере данных о

географии распространения и плотности непарного шелкопряда показывают значимость эффекта агрегированной группы для динамики вселившегося фитофага.

В нашем уравнении убыли два коэффициента смертности, прямо зависящего от плотности популяции α, и независимого β. Если α учитывает быстрейшее исчерпание необходимых для развития ресурсов по мере повышения числа личинок, то при низкой плотности достигших стадии размножения имаго *S* имеет смысл учитывать потери воспроизводства от неоплодотворенных самок. Дополним β в (3) функционалом:

$$\Psi(S) = 1 + \exp(-\sigma S^2), \lim_{S\to\infty} \Psi(S) = 1, \Psi(0) = 2. \quad (4)$$

Где $\sigma < 1$ отражает степень выраженность эффекта. Убывающий функционал быстро стремится к единице и далее не влияет на вычисление $N(T)$, когда численность продуцирующих поколение имаго соответствует среднемноголетнему оптимуму. Зависимость с учетом (4) получит дополнительное пересечение с биссектрисой, которое станет для динамической системы неустойчивым отталкивающим равновесием S^R, а точка начала координат (0,0) приобретет устойчивость: $\forall S < S^R : \lim_{t\to\infty} \{\varphi(S)\}^t = 0.$

Предлагаемый подход учитывает, что жизненный цикл вредителя включает метаморфозы между стадиями с разными физиологическими и экологическими особенностями. В работах о причинах вспышек изначально малочисленного насекомого отмечается, что для каждой стадии требуются определенные ресурсы и есть специфические хищники. Современные вычислительные средства позволят реализовать концепцию ступенчатого описания динамики поколения соответственно стадиям типичного вредителя с неполным циклом превращений: яйца, нимфы, имаго.

Подход заключается в организации алгоритма выделения метаморфоза как события, обусловленного достижением особого состояния в пространстве переменных непрерывной модели. Дискретные моменты событий разбивают время на последовательность кадров, в которых изменяется скорость убыли $N(t)$. Систему с динамически переопределяемой правой частью построим на основе модификаций (3) с условиями завершения активности каждой из форм правой части:

$$\frac{dN}{dt} = \begin{cases} -(\alpha_1 w(t)N(t) + \Psi\beta)N(t), & t < \tau \\ -\alpha_2 \Psi N(t)/w(\tau) - \beta N(t), & t > \tau, \\ -\alpha_3 w(t)N(t)N(t-\zeta), & w(t) < w_3, \end{cases} \quad (5)$$

где τ – длительность первой стадии с эндогенным питанием, далее модель описывает выживаемость стадии, где достигнутый показатель развития $w(\tau)$ уменьшает смертность, продолжающуюся по достижении порогового уровня w_3. В уравнение для старшей стадии развития введено небольшое запаздывание $\zeta < \tau$. Обосновано условиями задачи, что интервал действия зависящих от плотности факторов смертности не является постоянным и может растягиваться при замедлении скорости развития из недостатка ресурса. Популяция в период вспышки может состоять из совокупности нескольких одновременно живущих конкурирующих поколений $\mathbf{N} = \sum N_l, l \le 3$, но находящихся на разных стадиях развития.

Модель рассчитана на применение современных вычислительных средств, включающих библиотеки производительных численных методов с переменным шагом интегрирования. Алгоритмическая реализация непрерывно-событийной структуры вычислительной модели основаны на специально организованных структурах гибридного времени. Модель представляется конечным множеством режимов изменения состояния и переходов между ними. Переходам соответствует условие завершение активности и правило переопределения начальных условий для решения задачи Коши на следующем кадре времени с выбранным видом правой части.

Гибридное время формализуется в виде мультимножества, которое вводит компоненту событийности при управлении изменением непрерывного процесса:

$$\vartheta = \bigcup_n \{R_\tau_n, [t_{n-1}, t_n], L_\tau_n\}.$$

Где P_τ, L_τ – выделяемые события с мгновенной длительностью, ограничивающие справа и слева интервалы непрерывного времени.

В некоторый выделяемый момент гибридного времени происходит переопределение начальных условий для расчета задачи Коши на следующем в последовательности кадре непрерывного времени. Поведение гибридной системы «склеивается» из непрерывного изменения состояния и дискретных событий, переопределяющих развитие процесса.

Вычислительные средства для исследования предикативно переопределяемых гибридных систем в Санкт-Петербурге развиваются научными группами Ю.Б. Сениченкова и Ю.Б. Колесова [8]. Тестировать пригодность численных методов для задачи работы с гибридным временем можно по появлению так называемого «эффекта Зенона», когда некорректно работающий алгоритм останавливает время, и система будет бесконечно приближаться к точке перехода, подобно Ахиллесу пытающемуся догнать уползающую черепаху из известной апории греческого философа.

Нужно отличать гибридные системы от дискретно-событийном подхода, где происходят переходы между состояниями моделируемой системы согласно графу всех возможных состояний. В применяемом методе на основе таймированного гибридного автомата переключение реализуется между *режимами изменения* состояния. Режимам изменения сопоставлен набор форм правой части системы уравнений из (2), алгоритм контроля предикатов определяет выбор решаемой в данный момент задачи Коши с инициализацией новых начальных условий. Промежуток интервала развития вредителя разделен на последовательность кадров гибридного модельного времени. Алгоритмическое представление модели реализуется на основе автомата с таймированными и предикативными переходами. Множество решений задач Коши для допустимых $S \in Z^+$ определит интересующую нас зависимость, называемую в работах ихтиологов «кривой воспроизводства» популяции.

Исследование подобных гибридных моделей можно осуществлять в инструментальной вычислительной среде AnyLogic5 (к сожалению, разработчики отказались от развития данного направления в последующих версиях системы) и разрабатываемой в Санкт-Петербурге среде MvStudium в новой версии получившей название Rand Model Designer. Программный код выполняемой модели в Rand Model Designer генерируется на основе входного языка записи математической модели и визуальных диаграмм для описания структуры и качественных изменений поведения моделируемой системы и автоматически компилируется, что обуславливает высокую производительность при проведении управляемых вычислительных экспериментов. Входной паскалеобразный алгоритмический язык среды позволяет формировать модель процесса из алгебраических или дифференциальных уравнений и набора предикатов. Особенно ценна для автора возможность выполнять параметрическую оптимизацию моделей с использованием встроенных алгоритмов.

2. Анализ разработанной системы

Исследованная в инструментальной среде AnyLogic5 дискретная динамическая система организованная как $S_{n+1} = \varphi(S_n), S = N(T)$ продемонстрировала интересные для рассматриваемой популяционной задачи характеристики фазового портрета, так как кривая зависимости имеет локальные экстремумы, максимум и минимум, и четыре стационарные точки – пересечения с биссектрисой координатного угла.

Помимо известных изменений аттракторов для моделирования биологических процессов интересны трансформации, которые могут испытывать области их притяжения. Свойства зависимости приводят к тому, что первые три стационарные точки $S_1^R, S_2^R, S_3^R < S^*$ неустойчивы. Сохраняют притягивающие качества нулевое равновесие и устойчивая стационарная точка S^*. Границей их областей притяжения Ω_0, Ω_S согласно рис. 1 является первая стационарная (репеллерная) точка S_1^R. Поведение динамической системы с начальной точкой $S_0 \in (S_2^R, S_3^R)$ отличается от итераций Фейгенбаума, где траектория может притягиваться к точечному аттрактору в зависимости от значений параметра монотонно либо с затухающими осцилляциями [9].

У полученной функциональной зависимости выделяется интервал $(d_1, d_2) \subset [S_1^3, S_2^R], \varphi(d_1) = \varphi(d_2) = S_3^R$, который имеет свойство $\forall S \in (d_1, d_2)\ \varphi(S) > S_3^R$ и множество точек интервала A_1 монотонно притягиваются к S^* при первой итерации. Под действием следующей итерации некоторые начальные точки $S_0 \in (S_1^R, d_1) \cup (d_2, S_2^R)$ покидают интервал, которые составляют множество $A_2 = \left\{ S, S \in [S_1^R, S_2^R], \varphi^2(R) > R_3^R \right\}$. Существует инвариантное $\Delta = \left[S_1^R, S_2^R \right] \setminus \bigcup_{n=1}^{\infty} A_n$ множество не покидающих интервал под действием функциональных итераций точек и оно обладает аналогичной критическому канторовскому аттрактору структурой [10], что приводит к наблюдению временного апериодического движения для начальной точки $S_0 \notin \Delta$.

Так как $\max\varphi(S) > S_3^R$ у каждой из двух неустойчивых стационарных точек есть по две непосредственные точки прообраза, точек которые под действием итераций $\varphi^{-1}(R)$ должны отобразиться в S_3^R или S_2^R. У одной из точек прообразов $\varphi^{-1}(S_3^R) \in (S_2^R, R_3^R)$ будет три точки пробраза $\varphi^{-2}(S_3^R)$ Очевидно, так формируется замкнутое множество $\left\{\varphi^{-n}(S_2^R)\right\} \cup \left\{\varphi^{-n}(S_3^R)\right\}$ не принадлежат области притяжения аттрактора S^* и делающее его область притяжения Ω_S несвязным подмножеством. Траектория $\varphi^n(S_0)$, $S_0 \notin \Lambda$ испытывает апериодические флуктуации. Генерация транзитивного хаоса по терминологии [11] в модели происходит на ограниченном сверху уровне численности $\varphi^j(S_0) < \varphi(S_3^R)$ и конечна по времени.

Режим переходного или «транзитивного» хаотического поведения в вычислительном эксперименте на рис. 2 прерывается псевдостабилизацией, когда траектория оказывается в близкой точке неустойчивого равновесия $\varphi^{n+1}(S) \approx S_3^R$, но незначительные погрешности нарастают при итерациях и будут выталкивать траекторию из его ε-окрестности непредсказуемо в одну из сторон. Один из периодов ложного уравновешивания на некоторой итерации j завершится превышением порогового значения. Траектория окажется в непрерывной части области притяжения S^*, где быстро притягивается к устойчивому равновесию, характеризующему состояние популяции при высокой численности. Естественно, что продолжительность флуктуаций *j* изменяется в зависимости от выбора начальной точки.

Согласно предложенной модели развитию вспышки должен предшествовать период отчетливо видимой стабилизации на предпороговых значениях, который можно своевременно определить.

Работа выполнена в рамках проекта РФФИ №14-01-31020 для молодых ученых.

СПИСОК ЛИТЕРАТУРЫ

1. Barbosa P., Letourneau D., Agrawal A. Insect outbreaks revisited. Oxford: John Wiley & Sons, 2012, 492pp.
2. Криксунов Е.А., Снетков М.А. Модель формирования пополнения нерестового стада с учетом весового роста рыб // Доклады АН СССР, 1980, Т.253, №3, С.759–761.
3. Переварюха А.Ю. Эффекты и свойства нелинейных динамических систем в экологической интерпретации // Экологические системы и приборы, 2014, №7, С.31–38.
4. Kolesov Y., Senichenkov Y. Simulation of Variable Structure Models using Rand Model Designer // Proceedings of the 2013 8th EUROSIM Congress on Modelling and Simulation, P.294–299.
5. Gilpin M.E. Soulé M.E. Minimum viable populations: The processes of species extinctions // Conservation biology: The science of scarcity and diversity. Sunderland: Sinauer Associates, 1986, pp.13–34.
6. Keitt T.H., Lewis M.A., Holt R.D. Allee effects, invasion pinning, and species borders // The American Naturalist, 2001, Vol.157, №2, P.203–216.
7. Tobin P.C. The role of Allee effects in gypsy moth, Lymantria dispar (L.), invasions // Population Ecology, 2009, Vol.51, P.373–384.
8. Сениченков Ю.Б., Колесов Ю.Б., Инихов Д.Б. Формы представления динамических систем в MvStudium // Компьютерные инструменты в образовании, 2007, №4, С.44–49.
9. Feigenbaum M.J. The transition to aperiodic behavior in turbulent systems // Communications in Mathematical Physics, 1980, Vol.77, №1, P.65–86.
10. Graczyk J., Sands D., Swiatek G. Metric attractors for smooth unimodal maps // Annals of Mathematics, 2004, Vol.159, P.725–740.
11. Astafev G.B., Koronovski A.A., Hramov A.E. Behavior of dynamical systems in the regime of transient chaos // Technical Physics Letters, 2003, Vol.29, №11, P.923–926.
12. Dushoff J., Huang W., Castillo-Chavez C. Backwards bifurcations and catastrophe in simple models of fatal diseases // Journal of Mathematical Biology, 1998, Vol.36, P.227–248.
13. Пальникова Е.Н., Метелева М.К., Суховольский В.Г. Влияние модифицирующих факторов на динамику численности лесных насекомых и развитие вспышек массового размножения // Лесоведение, 2006, №5, С.29-35.
14. Clark L.R. The population dynamics of Cardiaspina albitextura (Psyllidae) // Australian Journal of Zoology, 1964, Vol.12, №3, P.362–380.
15. Odum E.P. Fundamentals of ecology. Philadelphia: Saunders, 1971, 574p.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 626.44

ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОЦЕССА СУДОПРОПУСКА ПУТЕМ УСТАНОВКИ НА СУДОХОДНЫЕ ШЛЮЗЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Абрашкин Анатолий Владимирович, Саушев Александр Васильевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, Двинская ул., д. 5/7
e-mails: Neyrogelos@yandex.ru, saushev@bk.ru

Аннотация: В статье рассмотрены перспективы развития автоматизированных информационно-управляющих систем для автоматизации процесса судопропуска и автоматизированные идентификационные системы, предназначенные для повышения эффективности и безопасности этого процесса.

Ключевые слова: *системы управления; судоходный шлюз; автоматизация.*

PROSPECTS OF DEVELOPMENT OF PROCESS OF SUDOPROPUSK BY INSTALLATION ON NAVIGABLE LOCKS OF THE AUTOMATED MANAGEMENT INFORMATION SYSTEMS

Anatoly Abrashkin, Alexander Saushev
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
e-mails: Neyrogelos@yandex.ru, saushev@bk.ru

Abstract: In article prospects of development of the automated management information systems for automation of process of a sudopropusk and the automated identification systems intended for increase of efficiency and safety of this process are considered.

Keywords: *a control system; navigable gateway; automation.*

Введение. В настоящие время актуальной является задача разработки и внедрения автоматизированных информационно-управляющих систем [1], [2] в составе систем мониторинга и управления гидротехническими сооружениями, предназначенными для процесса судопропуска.

Целями создания таких систем являются:

– внедрение инновационных технологий управления объектами технологической инфраструктуры канала;

– предупреждение аварийных ситуаций, связанных с работой оборудования сооружений;

– повышение безопасности [3];

– снижение времени простоя канала в случае возникновения нештатных ситуаций;

– лучшение качества обслуживания судов, проходящих по каналу и сокращение времени простоя судна.

Рассмотрим основные известные разработки таких систем.

Автоматическая идентификационная система

В настоящее время широко используется автоматическая идентификационная система (АИС) (Рисунок 1), предназначенная для повышения уровня безопасности мореплавания, эффективности судовождения и эксплуатации центра управления движением судов (ЦУДС), защиты окружающей среды.

Данная система обеспечивает выполнение следующих функций:

– предупреждение столкновений в режиме судно-судно;

– получение компетентными береговыми службами информации о судне и грузе;

– ЦУДС в режиме судно-берег для управления движением судов;

– мониторинг и слежение за судами, включая операции по поиску и спасанию.

Рис.1. Автоматическая идентификационная система

АИС включает в себя УКВ передатчик, один или два УКВ приёмника, приёмник GPS и приёмник глобальной спутниковой навигации (для России модуль ГЛОНАСС в приборе АИС является строго обязательным, основным источником координат. GPS), контроллер на основе микропроцессора, оборудование ввода-вывода информации на элементы управления.

Принцип действия АИС основан на приёме и передаче сообщений по УКВ волнам (Рисунок 2).

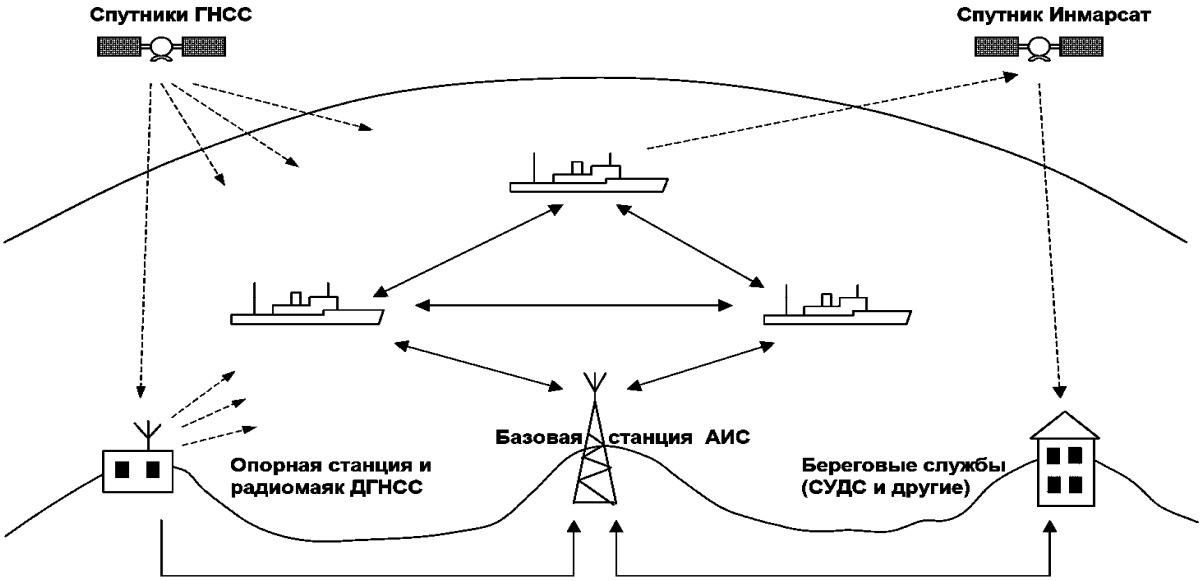


Рис.2. Принцип действия АИС

Передатчик АИС работает на более длинных волнах, чем радары, что позволяет производить обмен информацией на местности, имеющей препятствия. Система передает и получает информацию по двум радиоканалам для того, чтобы избежать проблем интерференции сигналов и не нарушать коммуникацию других объектов.

Сообщения АИС содержат:

– информацию об объекте, получаемую на основе использования методов идентификации;

– информацию о состоянии объекта, получаемую с элементов управления объектом;

– информацию о географических и временной координатах, которые АИС получает от глобальной навигационной спутниковой системы;

– информацию, вводимую вручную обслуживающим объект персоналом.

В Международном Регламенте Радиосвязи закреплено для использования в целях АИС два канала: AIS-1 (87В , 161,975 МГц) и AIS-2 (88В , 162,025 МГц). Скорость передачи цифровой информации в канале АИС выбрана 9600 бит/с.

Работа каждой станции АИС синхронизирована по времени UTC с погрешностью не более 10 мкс от приёмника ГЛОНАСС/GPS. Для передачи информации используются непрерывно повторяющиеся кадры длительностью 1 минута, которые разбиваются на 2250 временных интервалов по 26,67 мс.

Автоматизированная информационно-управляющая система

На сегодняшний день известны информационные системы, главной целью которых является отслеживание динамики движения судов, состояния судоходных каналов и гидротехнических сооружений.

Эти системы для каждого шлюза интегрируется в систему оперативно-диспетчерского управления гидросооружениями и судоходством, в состав которой входят Автоматизированные рабочие места (АРМ): главного диспетчера, диспетчеров судоходных каналов, а так же начальников вахт шлюзов.

Информационно-управляющие системы технологической безопасности судопропуска предназначены для:

– осуществления технологического процесса судопропуска, в том числе при наличии однократной неисправности, в автоматизированном режиме;

– реализации и контроля состояния блокировок безопасности и защитных блокировок;

– максимального снижения влияния «человеческого фактора» на безопасность судопропуска;

– осуществления видеонаблюдения всех этапов судопропуска;

– архивирования данных о процессе судопропуска, в том числе данных с видеокамер;

– взаимодействия с иными информационными и управляющими системами, такими как шлюз, канал в целом и т.п.

Система должна включать в свой состав целый ряд подсистем, выполняющие определенные функции. Рассмотрим основные из них.

АРМ диспетчера судоходного канала.

На мониторы автоматизированного рабочего места диспетчера канала выводится информация о типе, местоположении и параметрах движения судов по территории канала и на подходах к нему, уровне воды в бьефах и камерах шлюзов.

Информация на АРМ поступает с судна, оборудованного Автоматической идентификационной системой, находясь вблизи шлюза. При этом регулярно передается в диапазоне ОВЧ и УКВ частотах информация о судне, его координатах, курсе, векторе скорости, опасном грузе на борту, порте назначения, времени прибытия и т.д. Информация об уровне воды в бьефах шлюза поступает с датчиков, расположенных на самом шлюзе.

Основные выполняемые функции:

– автоматизированная подготовка распоряжений и указаний по процессу судопропуска для капитана судна;

– специализированное программное обеспечение для оптимизации процесса судопропуска через канал по критерию, учитывающему экономию энергоресурсов;

– фиксация всех действий о процессе судопропуска и работе оборудования в базе данных;

– автоматизированная подготовка отчетной и статистической информации для отправки в систему верхнего уровня.

Специализированные автоматизированные системы мониторинга (САСМ).

Данная система состоит из более простых подсистем, среди которых можно выделить:

1. САСМ службы автоматики

В состав САМС службы автоматики входят, вычислительная машина с данными о времени наработки до отказа, а так же вероятностью отказа оборудования установленного на шлюз и программным обеспечением для их автоматического расчета времени до отказа того или иного устройства.

Основные выполняемые функции:

– мониторинг работы электрооборудования и систем автоматики;

– автоматический подсчет наработки и остаточного ресурса всех элементов систем автоматики и силового оборудования;

– автоматизированное планирование и учет работ по обслуживанию оборудования.

2. САСМ службы механиков

Механикам поступают данные о состоянии передаточного устройства осуществляющие передачу механического усилия от двигателя к рабочим воротам и затворами водопроводных галерей. Также выводится информация о положении рабочих ворот и затворов водопроводных галерей, снимаемая с датчиков угла поворота.

Основные выполняемые функции:

– мониторинг параметров работы механического оборудования

– дистанционная диагностика состояния механизмов;

– автоматизированное планирование и учет работ по обслуживанию оборудования.

3. САСМ службы гидротехников

Эта система выдает данные о кривизне водного зеркала, уровне воды в нижнем и верхнем бьефах, текущем уровне воды в шлюзе и другие данные.

Основные выполняемые функции:

– мониторинг гидротехнических параметров сооружений канала;

– информирование о текущем состоянии шлюза капитана судна.

4. САСМ энергодиспетчера

Система мониторинга и контроля потребления энергоресурсов обеспечивает автоматический сбор и анализ данных с узлов учета. Она включает в себя данные об энергоснабжении шлюза, полученные с измерительных приборов.

Основные выполняемые функции САСМ энергодиспетчера:

– мониторинг работы систем энергоснабжения технологических объектов канала;
– дистанционное управление системами энергоснабжения объектов канала;
– мониторинг работы и дистанционное управление агрегатами насосных станций с учетом потребности водных ресурсов на судопропуск;
– контроль параметров внешнего энергоснабжения и учет потребления энергоресурсов;
– фиксация всех действий по работе оборудования в базе данных;
– автоматизированная подготовка отчетной и статистической информации.

Программный комплекс предназначен для: автоматического сбора информации с узлов учета; анализа полученных данных и выявления нештатных режимов работы узлов учета и установленного на них оборудования; предоставления отчетов энергопотребления (Рисунок 3).

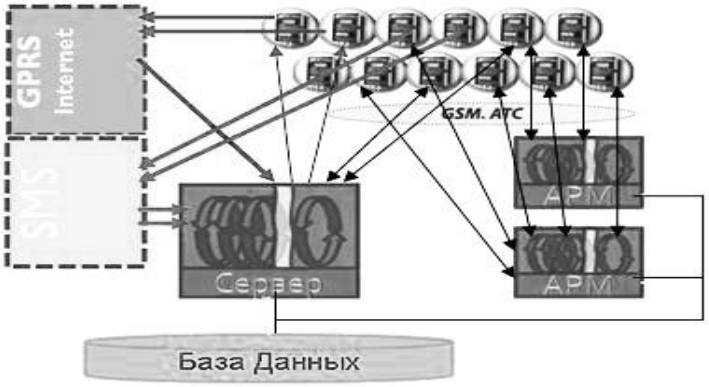


Рис.3. Система мониторинга и контроля потребления энергоресурсов

Рассмотрим структуру автоматизированной информационно-управляющей системы. Система делится на два уровня – нижний и верхний:

Автоматизированная информационная-управляющая система нижнего уровня (Рисунок 4) должна обеспечивать сбор информации с датчиков, установленных на шлюзе, и вывод этой информации на пульт управления диспетчера шлюза. Это позволит отслеживать параметры шлюза и своевременно предотвращать или устранять аварийные ситуации.

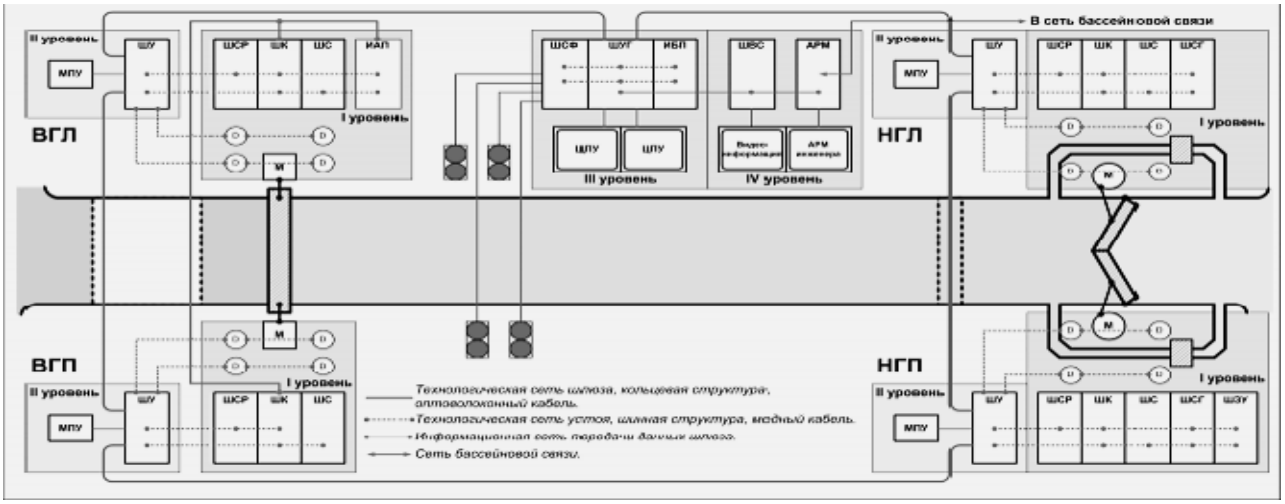


Рис.4 Автоматизированная информационная-управляющая система нижнего уровня

Информационно-управляющая система технологической безопасности судопропуска нижнего уровня строится по многоуровневой иерархической схеме.

Первый технологический уровень

В состав первого технологического уровня входят: технологические датчики, измерительные приборы и силовая исполнительная аппаратура.

В составе приводов ворот и затворов применены резервированные асинхронные электродвигатели, управляемые преобразователем частоты.

В состав сборок шкафов входят основной и резервный комплекты силового оборудования.

Контроль положения ворот и затворов осуществляется цифровыми датчиками, способными измерять положение с точностью до 0,05 мм.

Контроль нагрузки на механизмы осуществляется современными измерительными системами.

Второй технологический уровень

В состав второго технологического уровня входят: промышленные контроллеры, выполняющие программу управления исполнительными механизмами шлюза, местные пульты управления и модули передачи сигналов.

Контроль положения механизмов и управление силовым оборудованием осуществляет промышленный программируемый контроллер;

Система управления собрана по модульному принципу и обеспечивает возможность оперативной замены любого модуля без остановки технологического процесса.

Для проведения регламентных работ на механизме и местного управления применены релейный и цифровой пульты управления.

Третий технологический уровень

В состав третьего технологического уровня входят: центральный контроллер, выполняющий программу общесистемного управления шлюзом путем формирования заданий для контроллеров второго уровня и центральный пульт управления.

Центральный пульт управления содержит два сенсорных графических терминала.

Управление технологическим процессом шлюзования и контроль блокировок безопасности осуществляет резервированный промышленный программируемый контроллер.

Взаимодействие между контроллерами 2 и 3 уровней осуществляется через кольцевую сеть передачи данных.

Четвертый технологический уровень

В состав четвертого технологического уровня входят: видеосистема, обеспечивающая запись и хранение видеоархивов и АРМ инженера, предназначенный для настройки параметров ИУС ТБС.

На пульт инженера выводится вся необходимая информация для обслуживания системы и настройки параметров механизмов.

Система технологического видеонаблюдения позволяет производить круглосуточное наблюдение за процессом шлюзования.

Первые три уровня системы являются резервированными. Четвертый уровень системы, как правило, выполняется нерезервированным.

Автоматизированная информационная-управляющая система верхнего уровня предназначена для объединения всех шлюзов в одну единую информационную сеть. Это позволяет оптимизировать использование судоходных путей по критерию сокращения времени хода судов, которые будут перенаправляться на менее загруженные шлюзы. Кроме этого, система даст возможность задания капитану судна точного времени подхода к шлюзу, что позволяет уменьшить простои судов и расход топлива за счёт снижения скорости хода судна.

Заключение. Рассмотренные системы управления позволяют в той или иной степени повысить эффективность процесса шлюзования. Недостатком этих систем является отсутствие функций управления. Системы осуществляют только мониторинг и неспособны к предсказанию или предотвращению аварийных ситуаций и уменьшению очередей судов, ожидающих шлюзование.

В связи с этим возникает потребность разработки принципиально новой автоматизированной информационно-управляющей системы. Перспективным является синтез структуры системы автоматизации процесса судопропуска, учитывающей особенности рассмотренных выше систем управления, разработка и внедрение автоматизированной информационно-управляющей системы процесса судопропуска. Разработка и внедрение таких систем позволит сократить время перемещения судна из одной точки в другую; снизить расход топлива; обеспечить прогнозирование и своевременное устранение аварийных ситуаций.

Для достижения поставленной цели требуется решение комплекса технических задач, включающих: разработку на основе представленной концептуальной модели конкретных структурных схем нижнего и верхнего уровня; моделирование процесса судопропуска и разработку алгоритмического и программного обеспечения системы; решение оптимизационных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Саушев А.В. Основы управления состоянием электротехнических систем объектов водного транспорта: монография – СПб.; ГУМРФ имени адмирала С.О. Макарова, 2015, 222 с.
2. Бутин В.П. Повышение эффективности эксплуатации судоходных шлюзов на основе исследований, разработки и внедрения новых технических и технологических решений: автореф. дис. … канд. тех. наук. -СПБ, 1995. – 248 с.
3. Тарасов В.В. Обеспечение технологической безопасности судопропуска на Волго-Донском судоходном канале / В.П. Тарасов // ГИДРОТЕХНИКА XXI ВЕК. -2011. -№1 (4). -С 22 – 26.

УДК 681.2

РАНГОВАЯ ПАРТНЕРСКАЯ СЕРТИФИКАЦИЯ КАЧЕСТВА: КОНЦЕПЦИЯ, ТЕОРИЯ, ПРАКТИКА

Алексеев Анатолий Владимирович, Антипов Василий Васильевич,
Бобрович Владимир Юрьевич, Смольников Александр Васильевич
Институт автоматизации процессов борьбы за живучесть корабля, судна,
Санкт-Петербург, Россия, Ленинский пр., д. 101, оф. 162
e-mail: iapbgks@bk.ru

Аннотация: В статье рассмотрены тенденции развития систем сертификации соответствия и качества. Предложены новые концепция, теория и практика добровольной сертификации средств и аттестации объектов информатизации в рамках партнерских объединений добросовестных производителей. Отличительными особенностями предлагаемой технологии сертификации являются квалиметрическая оценка качества изделий и услуг, а также её ранжирование с открытой публикацией соответствующих подтверждающих документов, в том числе, в сравнении с национальным и международным уровнем технологического развития. В рамках предложенных концепции, теории и практики Ранговой партнёрской сертификации применительно к объектам морской техники и инфраструктуры показаны возможность реализации и апробированные технологии сравнительного анализа качества и повышения конкурентоспособности создаваемых изделий и услуг.

Ключевые слова: *информационные технологии, конкуренция, сертификация соответствия и качества, ранжирование, управление развитием, интеллектуализация управления.*

THE RANK OF PARTNER QUALITY CERTIFICATION: CONCEPT, THEORY, PRACTICE

Anatoly Alekseev, Vasily Antipov, Vladimir Bobrovich, Alexander Smolnikov
Institute of automation of processes of the struggle for the survival of the ship, vessel,
St. Petersburg, Russia, Leninsky prospect, D. 101, of. 162

Abstract: The article considers trends in the development of certification systems for compliance and quality. The proposed new concept, theory and practice of voluntary certification of funds and certification of Informatization objects within partnerships honest manufacturers. Distinctive features of the proposed technology certification are qualitative assessment of the quality of products and services, as well as its ranking with open publication of the relevant supporting documents, including in comparison with the national and international level of technological development. Under the proposed concept, theory and practice of Ranking partner certification for facilities related to marine engineering and infrastructure shown the feasibility and proven technology for comparative analysis of the quality and competitiveness of products produced and services.

Keywords: *information technology, competition, compliance certification and quality, ranking, development management, intelligent management.*

Актуальность оценки качества продуктов и услуг. 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 и морской инфраструктуры (ОМТИ) 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 [1], [2].

В этих условиях именно конкурентоспособность автоматизированных систем (АС) ОМТИ, 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 ОМТИ, а также как один из сильнейших маркетинговых аргументов [3], [4], [5].

Анализ тенденций и проблем развития систем оценки качества современных автоматизированных систем (АС) ОМТИ 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 ОМТИ [5], [6], [7].

Новая концепция. 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) [1], [2]. Прежде всего, объектов информатизации, как наиболее актуальных в условиях интенсивного развития современных информационных технологий и систем автоматизации.

В основе РПС лежит количественное измерение и ранжирование качества ОМТИ, как основной их системной характеристики. Практическое решение проблемы повышения качества создаваемых АС ОМТИ и их технологического развития на основе реализации концепции РПС, по нашему мнению, становится одним из наиболее доступных, реальных и системно целесообразных путей обеспечения конкурентоспособности АС ОМТИ, минимизации потребительского риска при их использовании и развитии.

В основу РПС в условиях действия Федерального закона «О техническом регулировании» и национальной концепции добровольной сертификации положены следующие принципы РПС:

– некоммерческого проведения сертификации изделий и услуг, формирования открытых баз данных и знаний по конкурентной способности сертифицированных средств;

– проведения квалиметрической независимой (объективной) и анонимной оценки качества изделий и услуг (количественного измерения качества) в рамках добровольных партнерских объединений добросовестных производителей с последующим ранжированием оценок качества и методически «прозрачным» определением уровня конкурентной способности;

– приоритетного использования технологий автоматической обработки результатов экспертного оценивания, независимой от негативного проявления субъективных (человеческих) факторов;

– открытости и прозрачности экспертного оценивания и документирования процедур РПС.

Другими отличительными признаками концепции РПС в сравнении с традиционными принципами сертификации соответствия изделий и услуг требованиям стандартов, регламентов и договоров являются:

– открытая публикация (прозрачность) соответствующих документов проведения сертификационных испытаний и фактически достигаемого при этом уровня качества;

– квалиметрическая оценка и публикация уровней конкурентной способности сертифицируемых изделий и услуг, в том числе, в сравнении с национальным и международным уровнями их технологического развития (сегодня этого практически нет);

– публикация соответствующих реестров сертифицированных средств и услуг с оценками достигаемых при этом уровней качества и конкурентной способности.

Таким образом, актуальность РПС в отличие от действующей системы сертификации (оценки соответствия требованиям стандартов, регламентов и договоров без оценок валидности изделий и услуг, т.е. количественной оценки степени достижения ими целей по предназначению) обусловлена: необходимостью перехода к квалиметрической (количественной) оценке и подтверждению соответствия продуктов и услуг (сертификации) достигаемому уровню качества и, как следствие, к оценке их конкурентной способности и преимуществ, в том числе, ранжированию полученных оценок в сравнении с национальным и международным (мировым) уровнем технологического развития.

Сущность концепции и технологии РПС. Основные положения концепции и технологии РПС в развитие [1], [2], [3], [4], [5], применимой как для систем автоматизации (СА), так и для других эрготехнических систем (ЭТС), в том числе, объектов морской техники и морской инфраструктуры (ОМТИ), иллюстрируются в структурно-графической форме, представленной на рисунке 1.

Рассмотрим конкретный вариант реализации концепции РПС ЭТС ОМТИ в судовых системах автоматизации, а также приведем достигаемые при этом преимущества и возможности обеспечения и повышения конкурентной способности создаваемых средств и систем автоматизации.

Среди преимуществ концепции РПС систем автоматизации ОМТИ применительно к системам комплексной судовой автоматизации, например, класса подсистем информационной поддержки судоводителей (СИП) [3], [4], [5], [6], [7], [8], следует выделить:

– прогрессивное саморазвитие и саморегулирование РПС (независимой и добровольной) за счет обеспечения условий равной конкуренции для участников некоммерческих классификационных партнерств (НП), формирования единых и достаточно простых условий и регламентов сертификации, а также существенно меньшего уровня стоимости РПС;

– квалиметрическое обеспечение оценивания конкурентоспособности изделий и услуг с «естественным» регулированием рынка и обеспечением адекватной защищенности потребителей;

– саморегулирование ценообразования объектов РПС и в целом ОМТИ, обоснованного уровнем достигаемого качества за счет информационной прозрачности для Потребителя (Заказчика) фактических значений уровня качества АС и их конкурентной способности;

– ускорение технологического развития объектов РПС за счет качественно нового уровня взаимного партнерского обмена технологической информацией и тем самым естественного мотивирования наращивания уровня качества изделий и услуг, конкурентной способности при контролируемом уровне информационного риска для членов НП.

ОСНОВНЫЕ ПОЛОЖЕНИЯ
Концепции ранговой (независимой, квалиметрической, добровольной) партнёрской сертификации АС и аттестации ОМТИ (Концепции РПС)

Основные понятия:

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Сертификация АС – деятельность (процесс) и форма подтверждения соответствия АС требованиям стандартов, технических регламентов (ТР) и договоров с соответствующей регистрацией результатов оценки соответствия.

Аттестация ОМТИ – освидетельствование объектов информатизации по требованиям ТР (регламентов, положений стандартов, условий договоров и т.п.) с соответствующей регистрацией.

Ранговая (квалиметрическая) партнёрская сертификация АС и аттестация ОМТИ (РПС) – деятельность (процесс) и форма количественной оценки (измерения) достигнутого уровня и ранга (степени) качества АС ОМТИ требованиям ТР с соответствующей их регистрацией и подтверждением.

Цели создания Системы партнерской (независимой, добровольной) ранговой (квалиметрической) сертификации и аттестации (СПРС):

- развитие требований государственной системы сертификации к качеству ЭТС ОМТИ
- обеспечение ускоренного технологического развития и конкурентной способности ЭТС
- формирование единого информационного пространства при управлении качеством ЭТС
- содействие Производителям и Заказчикам ЭТС в части прозрачности условий конкурирования
- минимизация рисков и обеспечение безопасности потребителей ЭТС ОМТИ

Организационная структура СПР

Коллегиальный сертификационный орган (КСО)

- формируется по представительскому принципу от членов НП
- принимает решения по введению в действие ТР, выдаче сертификатов
- собирается регулярно для утверждения решений ЦРПС и ПЭС

Центр ранговой партнерской сертификации (ЦРПС):

- организует деятельность СПРС: электронный документооборот (ЭДО); разработку нормативно-методической (НМД) и организационно-распорядительной (ОРД) документации;
- обеспечение деятельности ПЭС, КСО: регистрации заявок, сертификатов, ранжирования, аттестатов; организация контроля, надзора, рассмотрения апелляций; внешние связи; аннулирование сертификатов, аттестатов; информирование членов НП;
- ведение реестра сертифицированных ЭТС, квалиметрических БДЗ (КБДЗ);
- публикация ОРД, НМД, КБДЗ, положений о сертификации, аттестации, аккредитации, лицензировании

Партнерские экспертные советы (ПЭС):

- определение номенклатуры экспертируемых ЭТС и сегментов КБДЗ по ним;
- формирование и актуализация фонда ЭДО, КБДЗ по номенклатуре ПЭС;
- аттестация производства АС ОМТИ по данным сертификации СМК;
- согласование схемы, программ и методик (ПМ), состава комиссий;
- проведение сертификационных испытаний (СИ), протоколы и акт СИ;
- квалиметрическая оценка качества АС;
- подготовка проектов решений по сертификации и рангу качества АС, аттестации ОМТИ, предложений для КСО;
- рассмотрение апелляций, проведение инспекционного контроля

Заявители (разработчики, изго-товители, поставщики, потребители ЭТС ОМТИ):

- обеспечение соответствия ЭТС ОМТИ требованиям ТР;
- подготовка производства, стабильность характеристик ЭТС;
- сведения о сертифицированных ЭТС (их актуализация);
- маркировка сертифицированных ЭТС, уровня, ранга качества;
- применяют сертификат, знак соответствия, уровень качества;
- извещают о всех изменениях по сертифицированным ЭТС;
- обеспечивают беспрепятственный инспекционный контроль

Порядок проведения РПС ЭТС ОМТИ: регистрация заявки; аттестация производства АС; утверждение ПМ СИ; СИ; заключение по результатам СИ, достигнутому уровню и рангу качества; решение КСО; оформление сертификата качества, лицензии на знак и ранг качества; контрольный надзор; информирование; апелляции

Рис.1. Основные положения Концепции и технологии РПС ОМТИ

Методология РПС. В качестве методологической базы конкурентного сравнения объектов сертификации и аттестации с учетом [1], [2], [3] принят переход от подтверждения соответствия требованиям стандартов, регламентов и договоров (как это принято при традиционной системе сертификации СА и в целом ЭТС, аттестации ОМТИ) непосредственно к квалиметрической оценке (измерению) достигаемого уровня качества. При этом оценка качества производится с

использованием комплекса как частных (ЧПК), так и групповых (ГПК, отражают соответствующие свойства), и сводного (агрегированного) показателей качества (СПК) изделия или услуги. Именно это позволяет непосредственно переходить к сравнительной количественной оценке конкурентной способности и анализу конкурентных преимуществ разрабатываемых, используемых средств, систем и объектов автоматизации.

В свою очередь, это позволит совершенствовать сами процессы проектирования и выходить на высокие конкурентные уровни создаваемой продукции и предоставляемых услуг как на внутреннем, так и на внешнем рынке.

Важным методологическим вопросом взаимодействия членов НП при РПС является использование единых согласованных математических моделей сравнительной оценки качества оцениваемых технологических решений АС и средств её реализации. Это обеспечивает, с одной стороны, возможность методически прозрачной ранговой сертификации с квалиметрической оценкой достигаемого уровня качества и конкурентной способности средств, а, с другой стороны, верификацию и совершенствование разрабатываемых научно-методических аппаратов, их практическое и ускоренное внедрение и развитие. В том числе, в сравнении с корпоративными, национальном и международным (мировым) уровнем развития (в рамках альтернативных вариантов из состава непрерывно актуализируемой их базы данных и знаний).

Теория РПС. Базовые положения подобной математической модели и методологии применительно к РПС могут быть заимствованы из результатов [3], [4], [5], [6], [7], [8], прошедших достаточную апробацию и подтвердивших свою инвариантность к специфике целого ряда практических задач.

Ключевыми процедурами, методами и алгоритмами количественного анализа современных сложных по архитектуре и функциональным возможностям АС ОМТИ могут быть названы три модели: обеспечения инвариантности используемых ЧПК к специфике каналов измерения и контроля качества (модель инвариантного канала контроля ЧПК); обеспечения интегрированной оценки качества ЭТС (модель агрегирования показателей качества); обеспечения классификации состояний канала контроля качества (модель классификации состояний канала).

1. Математическая модель инвариантного канала контроля ЧПК при измерении любого из организационно-технических параметров АС ОМТИ (например, уровня давления, температуры, объема, стоимости устройств, уровня сертификации, степени выполнения регламентных работ и т.п.) в обобщенном виде может быть представлена следующим образом:

$$q_n^H = \left\{ \frac{[q_n - Min(q_n)]^h \times [Max(q_n) - q_n]^{1-h}}{Max(q_n) - Min(q_n)} \right\}^P, \qquad (1)$$

где: q_n^H – нормированное по алгоритму (1) значение ЧПК для измеряемого параметра q_n с номером n;

P – степень нелинейности шкалы оценок, равная $P = 1$ для линейных шкал и определяемая, в общем случае, по данным статистического анализа (при их отсутствии принимается значение $P = 1$);

$h = 1$ – позитивный характер связи измеряемого параметра с качеством ЭТС (например, прочность корпуса судна; надежность АС, дальность действия локатора, обобщенный уровень качества ЭТС по данным сертификации, комфортность принятия решений, уровень дизайна и т.п.);

$h = 0$ – негативный характер связи измеряемого параметра с качеством ЭТС (например, стоимость изделия, массогабаритные характеристики устройства, длительность восстановления, степень негативного влияния субъективных (человеческих) факторов, уровень риска (любого рода), длительность цикла обоснования и принятия управленческого решения и т.п.);

$Min(q_n), Max(q_n)$ – минимальное и максимальное значения диапазона изменения оценок ЧПК q_n при функционировании АС ОМТИ, определяемые, например, границами шкал приборов и т.п.

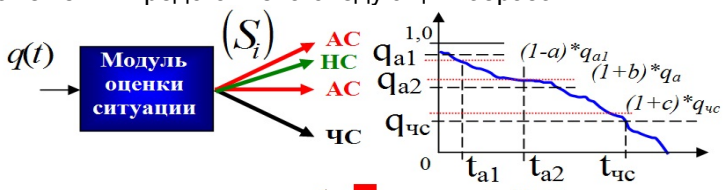
2. Математическая модель агрегирования показателей качества при оценке интегрированной оценки качества ЭТС при измерении комплекса организационно-технических параметров АС ОМТИ по частным показателям качества (ЧПК) и их агрегирования в групповые показатели качества (ГПК, характеризуют различные свойства АС в составе ОМТИ), а также агрегирования ГПК в модельные сводные показатели качества (МПК, определяются спецификой соответствующих моделей оценивания) и интегрированный СПК (характеризуют АС в целом), в обобщенном виде может быть представлена в виде, так называемого, гармонического алгоритма:

$$Q_n^Г = \left\langle \prod_{n=1}^{N} q_n^{\alpha_n} \times \sum_{n=1}^{N} (\alpha_n \times q_n) \right\rangle^{0,5}. \qquad (2)$$

Отличительным преимуществом гармонического алгоритма свертки ЧПК в ГПК, а также ГПК в МПК и МПК в СПК, следует считать промежуточное (компромиссное) значение получаемых оценок

СПК в сравнении с известными аддитивным (оптимистическим) и мультипликативным (пессимистическим) алгоритмами свертки. Это имеет особое значение для критических систем, в том числе, ОМТИ, при показателях ЧПК, ГПК и МПК в области малых значений, так как обеспечивает минимизацию погрешностей оценивания СПК.

3. Математическая модель классификации состояний инвариантного канала контроля качества при измерении любого из организационно-технических параметров АС ОМТИ (например, «соответствует заданным требованиям», «не соответствует заданным требованиям» и т.п.) в обобщенном виде может быть представлена следующим образом:



$$S\left[q(t),a,q_{a1},b,q_{a2},c,q_{\text{ЧС}}\right]=\begin{cases}\text{А1, если: } q_{a1}\le q(t)\le 1\\ \text{У1, если: } (1-a)\times q_{a1}\le q(t)\prec q_{a1},\ a\subseteq[0;1]\\ \text{НС, если: } (1+b)\times q_{a2}\prec q(t)\prec(1-a)\times q_{a1}\\ \text{У2, если: } q_{a2}\prec q(t)\le(1+b)\times q_{a2},\ b\subseteq[0;1]\\ \text{А2, если: } (1+c)\times q_{\text{ЧС}}\prec q(t)\le q_{a2},\ c\subseteq[0;1]\\ \text{УЧ, если: } q_{\text{ЧС}}\prec q(t)\le(1+c)\times q_{\text{ЧС}}\\ \text{ЧС, если: } 0\le q(t)\le q_{\text{ЧС}}\end{cases} \quad (3)$$

Применительно к названным выше задачам СИП обеспечения борьбы за живучесть судна состояние S_i инвариантного канала ЧПК *q(t)* в соответствии с алгоритмом (2) и пороговыми уровнями q_{a1}, q_{a2} , … классифицируется по поддиапазонам значений ЧПК следующим образом: НС – нормальное состояние (работа по штатному); У1, У2 – угроза аварийной ситуации (аварии) по верхнему (1) и нижнему (2) порогам; А1, А2 – авариная ситуация по соответствующим порогам (АС); УЧ – угроза чрезвычайной ситуации по нижнему порогу; ЧС – чрезвычайная ситуация.

Аналогичным образом состояние инвариантных каналов контроля качества АС ОМТИ классифицируется для групповых (ГПК), модельных (МПК) и сводного (СПК) показателей качества.

Практика реализации концепции РПС. К настоящему времени в ходе решения ряда практических задач накоплен определённый опыт и отработан ряд практических вопросов реализации излагаемой концепции и технологии РПС систем автоматизации ОМТИ в процессе:

– формирования квалиметрической базы данных и знаний (КБДЗ) альтернативных технологических решений (ТР, включая патенты, изобретения, полезные модели, описания ТР по данным НИР и ОКР, статьи и т.п.) в классе систем информационной поддержки борьбы за живучесть корабля, судна (более 200 альтернативных технологических решений) [3, 6-8];

– экспертного оценивания альтернативных ТР с использованием специально разработанных программных комплексов и методик оценивания «КРОПУР», «СППР ЭО», «БДЗ-БЖ», «МКО», «МКО-И» [9-12]. Основные фрагменты технологии экспертного оценивания ТР с использованием программного комплекса АСППР ЭО ТР «МКО-И» (версия «МКО-БЖКС») приведены на рисунке 2;

– автоматического формирования при реализации РПС комплекта документов: Заявителя (заявки на РПС в комплекте); Коллегиального сертификационного органа (КСО: решений о составе Партнерских экспертных советов (ПЭС) о возможности выдачи сертификата качества, сертификата качества ЭТС, реестра сертифицированных средств и т.п.); Центра РПС (ЦРПС: программ и методик, протоколов, акта проведения сертификационных испытаний и других); ПЭС (протоколов экспертного оценивания, автоматической оценки СПК, формирования и актуализации фонда электронного документооборота, квалиметрической базы данных и знаний (КБДЗ) по номенклатуре ПЭС и других);

– практической отработки регламентов проведения заседаний ПЭС, а также проведения публичных групповых экспертиз качества ЭТС, открытых заседаний ПЭС и других;

– открытой публикации материалов проведения РПС и публичного обсуждения концепции, технологии и практики квалиметрического сравнения технологических решений и оценки и конкурентной способности в реальных условиях анализа сложных ЭТС, в том числе класса СИП.

Так в апреле 2014 г. весьма успешно была проведена РПС в рамках Некоммерческого партнёрства «Институт автоматизации процессов борьбы за живучесть корабля, судна (ИАП БЖКС)». Экспертиза заявленных ТР была проведена в специальном формате сертификационных испытаний ЦРПС с открытым заседанием Партнерского экспертного совета по рассмотрению результатов оценки конкурентной способности технологических решений класса «Системы информационной поддержки решений по управлению сложными эрготехническими системами повышенного риска».

При этом заявители представляли свои предлагаемые ТР в форме как заявочного комплекта документации, так и обязательных 10-минутных презентаций ТР с обоснованием заявляемого уровня конкурентной способности в безличной (анонимной) форме. Далее следовали индивидуальная (независимый, анонимная) экспертиза каждого ТР с использованием специально разработанных

программных комплексов в защищенном исполнении и коллегиальное утверждение автоматически подготовленных протоколов и проекта решения Партнерского экспертного совета. Наконец, результаты сертификации качества ТР и оценки их конкурентной способности были публично оглашены и одобрены в рамках проводимого ИАП БЖКС цикла научно-практических семинаров.

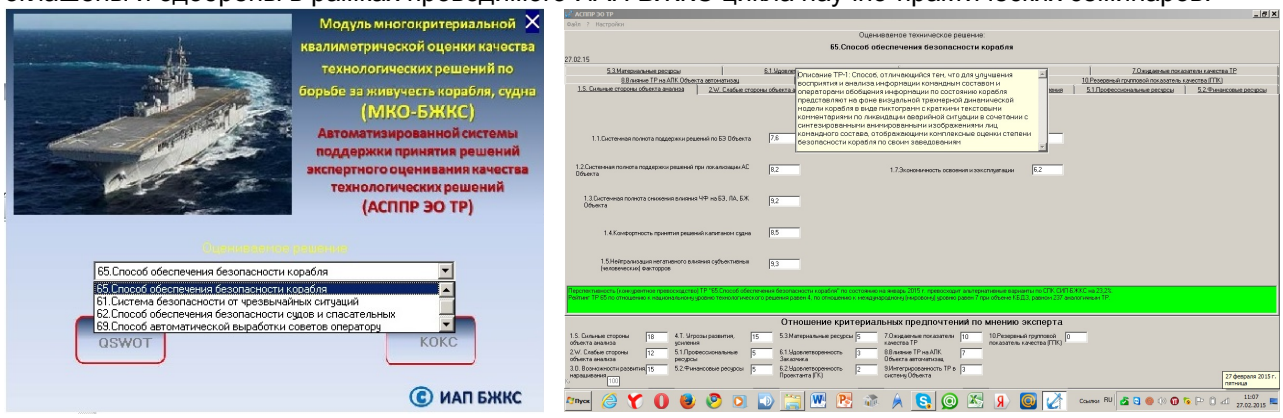


Рис. 2. Основные фрагменты технологии обеспечения экспертного оценивания СИП-БЖКС при использовании АСППР ЭО ТР «МКО-И»: выбор ТР; экспертная оценка ТР «65.Способ обеспечения…»

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 ОМТИ 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.

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 [12].

Выводы и рекомендации. Сегодня, при определенном дефиците конструктивных путей решения национальной проблемы повышения технологического уровня создаваемых технических комплексов и систем, обеспечения их конкурентоспособности, в качестве одного из перспективных путей и способов решения данной проблемы следует рассматривать переход к предложенной концепции и технологии РПС ЭТС и, особенно, критических ЭТС, включая ОМТИ.

Рассмотренные концепция, теория и практика 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 конкурентноспособных эрготехнических комплексов и систем, в том числе, автоматизированных систем управления объектов морской техники и инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Смольников А.В, Алексеев А.В., Антипов В.В., Бобрович В.Ю. Ранговая сертификация современных эрготехнических систем, как реальный способ повышения конкурентоспособности объектов морской техники и морской инфраструктуры – Морской Вестник, 2013, № 2 (14).
2. Смольников А.В., Алексеев А.В., Антипов В.В., Бобрович В.Ю. Пути повышения конкурентной способности объектов морской техники и морских транспортных систем на основе создания баз данных и знаний технологических решений и их ранговой сертификации / Вторая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем» ИКМ МТМТС 2013. Санкт-Петербург, 03-04 июля 2013 года. - ИКМ МТМТС 2013 – SCM MEMTS 2013, с. 109-114.
3. Смольников А.В., Сус Г.Н., Ушакова Н.П., Алексеев А.В. К вопросу выбора агрегированного векторного критерия оценки качества системы борьбы за живучесть объектов морской техники – Первая научно-практическая конференция «Современные технологии автоматизации борьбы за живучесть» – ИАП БЖКС, НПО «Аврора», 6.12.2012, ISBN 978-5-901218-15-0, с. 12-13.
4. Управление качеством высшего образования: теория, методология, организация, практика (Коллективная научная монография). Под научной ред. А.И.Субетто. – СПб.: Смольный институт РАО; Кострома: Изд-во КГУ, 2005. – В 3-х тт. – Т.1. – 406 с.
5. Алексеев А.В. Сертификация систем обработки информации. – СПб.: СПбГМТУ, 2010. – 159 с.
6. Алексеев А.В. Алгоритмическое обеспечение оценки качества сложных эрготехнических систем типа судов повышенного риска / Региональная конференция (РИ-2012). Юбилейная XIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. \ СПОИСУ. – СПб, 2012, с. 152-153.
7. Алексеев А.В. Технология и программный комплекс квалиметрической ранговой оценки качества сложных информационно-аналитических систем / Материалы IX Всероссийской научно-практической конференции МОРИНТЕХ-ПРАКТИК «Информационные технологии в судостроении–2008». – СПб., ОАО «Северные верфи»,19.06.2008, с.110-118.
8. Алексеев А.В. Алгоритмическое обеспечение оценки качества сложных эрготехнических систем типа судов повышенного риска / Региональная конференция (РИ-2012). Юбилейная XIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. \ СПОИСУ. – СПб, 2012, с. 152-153.
9. Смольников А.В., Алексеев А.В. Программа квалиметрической ранговой оптимизации проектных и управляющих решений (КРОПУР) - Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2013612649, 11.03.2013 (24.01.2013).
10. Смольников А.В., Алексеев А.В. Программа квалиметрического анализа и оценки конкурентноспособности технологических решений по информационной поддержке принятия решений судоводителем (QSWOT) - Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2013612929, 18.03.2013 (21.01.2013).
11. Смольников А.В., Алексеев А.В., Марченко А.В. Программный модуль экспертного квалиметрического оценивания уровней технологических решений по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля, судна (МКО)» - Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2014613608, 31.03.2014 (06.02.2014).
12. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор». Спб., 7-9.10.2014 – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С. 29-34.

УДК 681.2

ТЕХНОЛОГИИ МОНИТОРИНГА И УПРАВЛЕНИЯ ЗАЩИЩЕННОСТЬЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И ИНФРАСТРУКТУРЫ

Алексеев Анатолий Владимирович, Тюрин Иван Сергеевич,
Санкт-Петербургский государственный морской технический университет,
Санкт-Петербург, Россия, ул. Лоцманская, дом. 3,
e-mail: iapbgks@bkl.ru

Аннотация: В статье рассмотрены результаты анализа технологий мониторинга защищенности информационных ресурсов объектов морской техники и морской инфраструктуры, предложена новая концепция, а также описан созданный базовый вариант макетного действующего образца интегрированной системы автоматического управления информационной безопасностью, позволяющего выполнять оперативный системный мониторинг и эффективное управление защищенностью ИР в соответствии с изложенным подходом.

Ключевые слова: *информационная система; ресурсы, защищенность, интеллектуализация.*

TECHNOLOGY MONITORING AND MANAGEMENT OF SECURITY INFORMATION RESOURCES OF INTEREST FOR MARINE ENGINEERING AND INFRASTRUCTURE

Anatoly Alekseev, Ivan Tyurin,
St. Petersburg State Marine Technical University,
Russia, Lotsmanskaya Street 3, St. Petersburg.

Abstract: In the article the results of the analysis of monitoring technologies protection of information resources of interest in marine engineering and marine infrastructure, proposed a new concept, and describes the basic variant model of the current sample of the integrated system of automatic information security management, allowing to perform an online system monitoring and effective management of the security of IL in accordance with the above approach.

Keywords: *information system; resources, security, intellectualization.*

Автоматизация процессов защиты информации объектов морской техники и морской инфраструктуры (ОМТИ) в последнее время все чаще рассматривается в качестве наиболее критической и специфической задачи для аналогичных объектов и, особенно, в условиях ведения современных информационных и сетецентрических противоборств [1], [2], [3].

Среди проблемных вопросов в этой области сегодня одно из ключевых мест, по нашему мнению, занимает комплекс вопросов оценки, контроля и мониторинга состояния защищенности информационных ресурсов (ИР), а также эффективного управления ими [4], [5], [6].

Среди основных причин этого, прежде всего, могут быть названы [4], [5]:

– отсутствие сравнительных доверительных данных по рекомендуемым и практически используемым сертифицированным средствам оценки и контроля состояния защищенности ИР;

– практическое отсутствие методологии, технологий и средств мониторинга (наблюдения) состояния защищенности ИР, работающих в реальном масштабе времени (РМВ);

– фактическое отсутствие теоретических и методических общепризнанных положений по технологиям оценивания качества информационной безопасности (ИБ) объектов информатизации, включая ОМТИ, в первую очередь, по таким системным критериям, как конфиденциальность (Ки), доступность (Ди), целостность данных (Ци), а также по их агрегированному критерию – сводному (агрегированному) показателю качества ИБ [4], [6];

– невозможность, как следствие выше названного, эффективного, а, там более, оптимального оперативного управления процессами обеспечения безопасности информации (ОБИ) объектов информатизации типа ОМТИ, включая своевременное реагирование на возникновение информационных инцидентов, управление ими и их предупреждение [7];

– технологическая неготовность в настоящее время служб безопасности, в первую очередь, критических объектов, к числу которых в полной мере относятся ОМТИ, к ведению количественного мониторинга в РМВ и прогнозированию состояния защищенности ИР (ПЗР).

Вместе с тем, справедливости ради следует отметить, что к числу объективных факторов данных аспектов современного состояния проблемы технологического развития мониторинга защищенности ИР современных сложных эрготехнических систем и объектов информатизации, включая ОМТИ, относятся сравнительная новизна и значительная интенсивность развития в целом информационных технологий (ИТ), их многообразие на рынке ИТ, существенные наукоёмкость и ресурсоёмкость, определенная технологическая зависимость от центров мирового развития ИТ и др.

Для анализа состояния развития и специфических свойств технологий мониторинга защищенности ИР нами были протестированы демоверсии наиболее перспективных программных комплексов (ПК), включая современные средства анализа и мониторинга защищенности ИР типа: «Symantec Endpoint Protection 12.1.4», «Kaspersky System Management», «ESET NOD32 Smart Security Business Edition 5.0». А также более ранние представители этого класса средств защиты информации типа: «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».

На рисунках 1–3 приведены типовые варианты визуализации данных мониторинга и управления защищенностью ИР применительно к типовым условиям ОМТИ класса «Автоматизированное рабочее место (АРМ) администратора ИБ проектно-конструкторского бюро» при использовании известного программного комплекса (ПК) «10-Страйк: Мониторинг Сети» [8]. Он позволяет осуществлять мониторинг АРМ, серверов, принтеров и других устройств (хостов).

ПК периодически проверяет хосты путем отправки специфических запросов заданным сервисам, подключенным к портам и многими другими способами, реагируя на события от показа сообщения до перезапуска службы. ПК сканирует каждое АРМ в составе сети и интегрированной автоматизированной системы в защищенном исполнении (АСзи), автоматически получает перечень доступных хостов, формирует иерархический список мониторинга, назначает найденным хостам проверки по умолчанию, позволяет добавлять другие проверки, осуществляет постоянный мониторинг сервисов типа: TCP-порт, ICMP-пинг, DNS, ARP, SNMP, FTP, HTTP и другие [8].

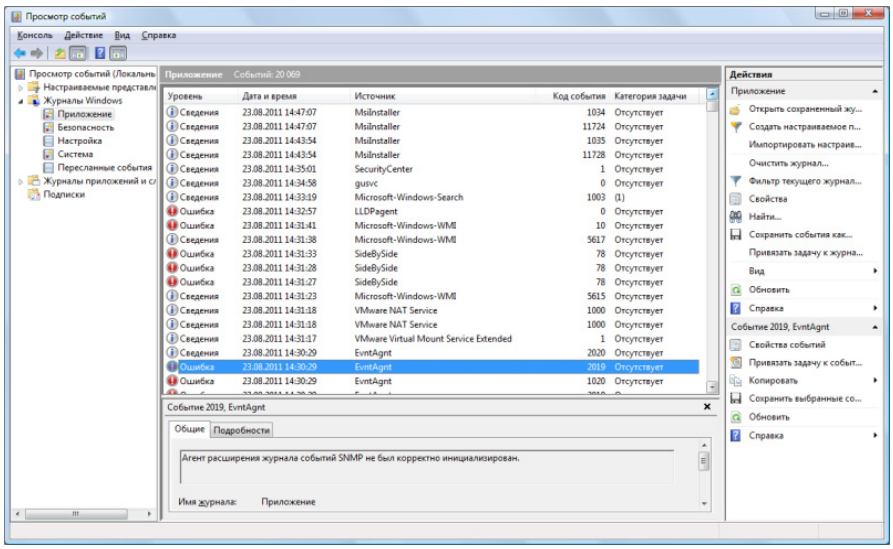


Рис. 1. Главная экранная форма АРМ администратора ИБ на базе ПК «10-Страйк»

На рисунке 2 приведена экранная форма ПК «10-Страйк» в режиме мониторинга трафика и анализа сетевой активности с возможностью обращения и анализа каждого из них.

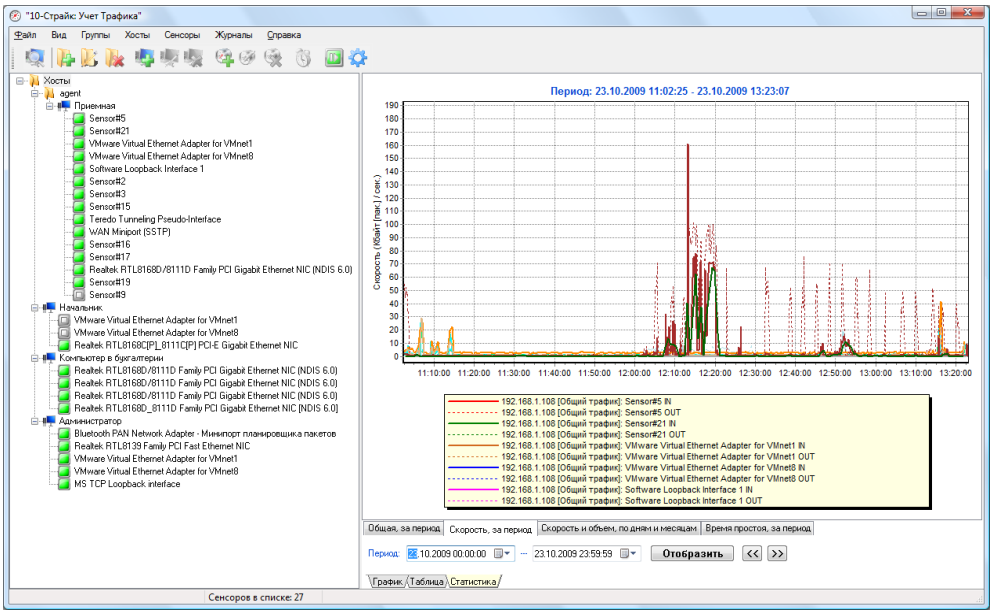


Рис. 2. Экранная форма ПК «10-Страйк» в режиме мониторинга сетевой активности

Вместе с тем, выполненный многовариантный анализ показал, что ни один из рассмотренных ПК практически не обеспечивает комплексный мониторинг состояния ИБ объектов информатизации, включая ОМТИ, в реальном масштабе времени, что в сочетании с многообразными, но мало структурированными вариантами визуализации данных существенно ограничивает его возможности.

Кроме того, при наличии широких возможностей информационно-аналитической поддержки (многочисленные графики, таблицы и тому подобные сервисы) весьма ограниченные возможности интеллектуальной поддержки принятия решений администратора ИБ (представление в автоматическом режиме рекомендаций и вариантов принятия решений) в условиях сложности структур АСзи и высокой динамики информационных процессов, прежде всего, в условиях информационных, сетецентрических вторжений и противоборства, создают для администратора ИБ весьма сложную ситуационную и психофизиологическую обстановку. Подчас это «приводит» его к чрезвычайному для управления АСзи состоянию, называемому часто «отказ от принятия решений».

Аналогичные сделанному выводы следуют из анализа технологических возможностей также другой из наиболее совершенных систем мониторинга состояния по ОБИ АСзи на базе ПК «Symantec Endpoint Protection 12.1.4» [9], главная экранная форма которого приведена на рисунке 3.

На главной экранной форме приведены основные показатели безопасности сети, а также обобщенное состояние защищенности сети в данный момент времени. Кроме того, приведены данные активности вредоносных кодов (вирусов), а также состояние компьютеров в сети. В данном

ПК предусмотрена также возможность настройки политик безопасности локально-вычислительной сети и уведомлений на телефон, в приложении и на почтовый сервис (e-mail).

Контроль за самой сетью осуществляется путем опроса АРМ об их состоянии за счет предустановленной программы-клиента, связанной с основным ПК «Symantec Endpoint Protection 12.1.4». ПК позволяет также просматривать отчеты и уведомления об ошибках или угрозах. Это дает общее представление о состоянии сети, но не позволяет быстро, в РМВ реагировать на них. Последнее, как уже отмечалось выше, является характерным для используемых сегодня технологий.

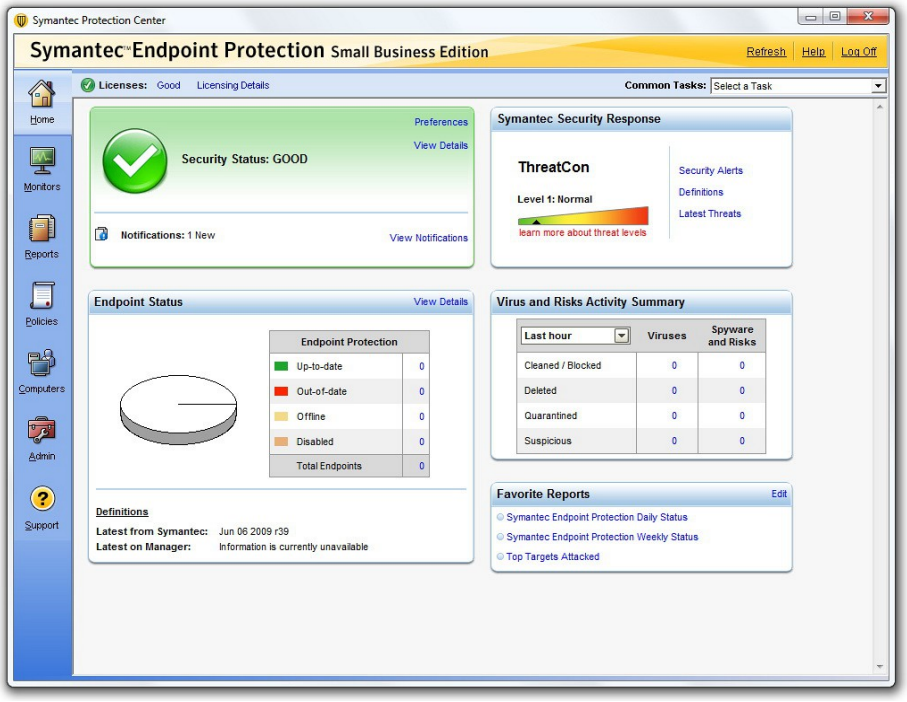


Рис. 3. Главная экранная форма АРМ администратора ИБ на базе ПК «Symantec Endpoint Protection 12.1.4»

В этих условиях, как никогда ранее, возникает актуальная задача системного исследования интегральных свойств и характеристик АСзи сложных систем и объектов типа ОМТИ в РМВ.

Существенно различающиеся между собой по построению, реализуемому функционалу рассмотренные ПК мониторинга защищенности ИР практически, как ни странно, не имеют единых критериев оценивания качества защиты ИР. Более того, ни один из них не обеспечивают оценку, контроль и мониторинг защищенности ИР по таким общепризнанным регламентированным требованиям и критериям, как конфиденциальность, доступность, целостность ИР (Ки, Ди, Ци).

При этом, наиболее распространенными подходами к оценке защищенности ИР и критериями используются: наличие сертификатов соответствующих видов; качество и своевременность (оперативность) решения задач анализа уязвимостей, TCP и UDP-сканирования, качество интерфейса для оперативного управления ОБИ, стоимость владения ПК; требуемые ресурсы памяти; цикл актуализации базы данных; состояние программы на конечной точке; регламент лицензирования, типы контролируемых ошибок (установки ПО, обновления ПО, ошибки неизвестных устройств и т.д.). Так, оценка степени защищенности ИР по названным критериям (выдача отчетов) производится, как правило, за интервал времени порядка 1 часа, что не позволяет управлять ОИБ в реальном масштабе времени и является весьма существенным ограничением [8], [9].

Более того, предлагаемый при этом набор графических форм представления данных анализа состояния защищенности ИР не предусматривает, как правило, непрерывность наблюдения (мониторинг) за соответствующими показателями, анализ трендов соответствующих характеристик. Тем самым, полезность представляемых данных (ценность информации, например, по критерию А.А. Харкевича) резко ограничивается невозможностью своевременного (оперативного) их использования в интересах нейтрализации уязвимостей и воздействия угроз на ИР. Тем более, для прогнозирования развития данных и обстановки на интервале времени до (20…30) минут и более.

С другой стороны, накапливаемые в процессе использования названных ПК данные по уязвимостям ИР, включая от вредоносных кодов, по потенциальным и реализуемым информационным вторжениям требуют существенного временного ресурса для ретроспективного анализа, выработки вариантов управленческих решений, а, тем более, для их реализации. Практически это приводит к «информационной перегрузке» администратора ИБ, проявлению негативного влияния его субъективных (человеческих) факторов (ЧФ), вплоть до такой информационно-управленческой уязвимости, как «отказ от управления».

В этих условиях, представляется актуальной новая постановка задач мониторинга защищенности ИР и в целом ОБИ объекта информатизации типа ОМТИ, которая включает:

– разработку концепции (концептуальное проектирование), методологии и технологии создания интегрированных систем автоматического управления (ИАСУ) ИБ объектов информатизации (формирования концепции создания ИСАУ ИБ);

– реализацию в составе ИАСУ ИБ функций и задачи системной квалиметрической оценки, контроля и мониторинга состояния защищенности ИР, причем, в отличие от традиционных технологий мониторинга не только по частным показателям качества (ЧПК типа выше названных), но и по групповым показателям качества (ГПК типа Ки, Ди, Ци), а также по модельным показателям качества (МПК типа сводный/агрегированный (СПКm /АПКm) по соответствующим моделям оценивания при их общем числе M, причем m = 1, 2, 3, …M, а также по интегрированному показателю качества типа СПК/АПК;

– реализацию задачи визуализации данных наблюдения в структурированном (системно-техническом) формате с нетрадиционным отображением наряду с непосредственно измеряемым множеством {ЧПКn} при их общем числе N, также аналитических данных типов {ГПКg} при их общем числе G, {АПКm} и АПК для их непосредственного использования при оценке обстановки администраторами ИБ, формировании ряда альтернативных проектов решений и принятия лучшего (оптимального) из возможных альтернативных вариантов решений непосредственно управленческого решения;

– реализацию задачи прогнозирования развития множеств {ЧПКn}, {ГПКg}, {АПКm}, АПК для каждого альтернативного варианта из общего их числа A, например, на основе технологий регрессионного анализа данных с оценкой параметров функций регрессии (трендов);

– реализацию задачи прогнозирования развития комплекса наблюдаемых параметров (ситуаций в целом) $\{S_z\}$ при их общем числе Z для каждого альтернативного варианта из общего их числа A, например, на основе технологий ситуационного анализа, ассоциативного анализа, интуитивного анализа, анализа образов и т.п. с оценкой соответствующих параметров ситуаций;

– реализацию задачи прогнозирования развития ситуаций на базе множества ранее полученных и отображаемых данных, например, на основе алгоритма (как один из несложных вариантов) выбора из базы данных и знаний (БДЗ) альтернативной ситуации с минимальным отклонением (отличием по комплексу параметров) от текущей (оцененной) ситуации;

– реализацию в дополнение к информационной и информационно-аналитической задачи интеллектуальной поддержки принятия решений администратором ИБ (офицером по ИБ) на основе автоматического анализа и оценки обстановки с выдачей (визуализацией, отображением) ранжированного по критерию $Max\{АПК_p\}$ (с наибольшими значениями АПК) ограниченного (порядка 3…5) ряда альтернатив из их множества при общем числе P;

– реализацию задачи традиционной регистрации данных наблюдения по многочисленному ряду показателей качества с нетрадиционным вариантом их визуализации кроме, как по ЧПК, также по ГПК, МПК и АПК (аналогов подобного варианта мониторинга в настоящее время не выявлено) и, непосредственно, по принятой в качестве оптимальной альтернативе решения;

– реализацию задачи автоматического формирования типовых (из БДЗ) управленческих команд с контролем их прохождения по каналам их доведения до исполнителей с последующим мониторингом исполнения управленческих команд в каждом из контуров управления. При этом предусматривается возможность перехода от автоматического варианта (режима) управления к автоматизированному за счет соответствующих корректирующих действий администратора ИБ;

– реализацию задачи комплексной апостериорной оценки качества принятых решений администратором ИБ объекта информатизации, а также их исполнения в интересах оценки эффективности управления (степени реализации проектного качества), актуализации данных, формирования когнитивных данных в соответствующей системе управления БДЗ.

В ходе проведенных к настоящему времени в Санкт-Петербургском государственном морском техническом университете и НП «ИАП БЖКС» специальных научных исследований подобная концепция сформирована применительно к задаче управления защищенностью ИР ОМТИ.

В её развитие выполнено тестирование, многовариантные квалиметрические оценки и рейтинг-анализ практически всего спектра специальных технических средств защиты информации из состава государственного реестра сертифицированных средств, который, в первую очередь, показал острую необходимость разработки методологии их системной интеграции применительно к типовым задачам ОМТИ [10], [11], [12], [13]. При этом, ключевым элементом и системообразующим элементом является подсистема мониторинга и управления защищенностью ИР ОМТИ на качественно новом уровне с решением приведенных выше задач.

В соответствии с этой концепцией были созданы базовый технологический образец и макетный действующий образец (МДО) ИСАУ ИБ в варианте системы поддержки решений и управления (СПРУ-ИБ), позволяющего выполнять оперативный системный мониторинг и эффективное управление защищенностью ИР в полном соответствии с изложенным подходом.

Применительно к ОМТИ типа судостроительное предприятие из [6] приведена главная экранная форма АРМ админи-стратора безопасности при реализации технологического образца ИСАУ-ИБ (вариант «СПРУ-ИБто»).

Структура видеокадра АРМ администратора безопасности включает 3 основных сегмента:

– в левой верхней части – сегмент двухбитовой визуализации состояния защищенности ресурсов предприятия по основным структурным элементам системы и службы безопасности, включая локально-вычислительную систему предприятия (1.ЛВС в части защищенности средств и ИР (1.1.ЗС), конфиденциальности (1.2.К), целостности (1.3.Ц), доступности (1.4.Д) ресурсов, несанкционированного доступа (1.5.НСД) к ИР), комплекса инженерно-технической защиты (2.Инж-тех), системы тревожно-охранной и пожарной сигнализации (3.СТОПС), системы управления, оповещения и связи (4.СУОС), системы охранного телевизионного наблюдения (5.СОТН), технического центра безопасности (6.ТЦБ), системы контроля и управления доступом (7.СКУД). В основу принципов, алгоритмов, организации и технологии мониторинга состояния безопасности предприятия положен опыт создания и эксплуатации технической системы безопасности ОАО «Кировский завод» [13], [14];

– в правой верхней части – сегмент мультиэкранной визуализации мониторинга обстановки с использованием данных системы охранного (с автоматическим выводом тревожных ситуаций) телевизионного наблюдения (5.СОТН);

– в центральной части – сегмент двухбитовой визуализации мониторинга (наблюдения во времени с циклом управления порядка 2 минут) состояния названных выше структурных элементов системы безопасности предприятия. Текущий момент времени (2:10) выделен желтым цветом. Интервал времени от 2:10 до 2:30 представлен результатами прогнозирования развития обстановки на основе использования полимодельных алгоритмов регрессионного анализа [6];

– в правой нижней части – всплывающий сегмент варианта проекта управленческого решения (ПУР) с автоматической регистрацией времени выработки ПУР, зарегистрированного исходного события, результата автоматической оценки обстановки, теста ПУР, фиксации времени принятия администратором предложенного ПУР (принятия решения), фиксации времени доведения решения до исполнительного элемента (органа), фиксации времени исполнения решения.

Применительно к системе обеспечения ИБ крупномасштабного ОМТИ типа «Морской флот РФ» (включающего Балтийское, Мурманское, Архангельское и другие пароходства) приведена главная экранная форма АРМ администратора ИБ в составе «СПРУ-ИБто».

В соответствии с сформулированной концепцией и информационной технологией мониторинга и управления защищенностью ИР из [13] приведена главная экранная форма макетного действующего образца АРМ офицера по ИБ в варианте системы поддержки решений и управления «СПРУ-ИБ» применительно к специфике условий защиты ИР автоматизированной системы в защищенном исполнении (АСзи) самоподъемной буровой установки.

При этом, АСзи представлена в составе семи основных подсистем обеспечения ИБ: подсистемы мониторинга защищенностью и управления безопасностью (1.ПМУБ), подсистемы разграничения доступа (2.ПРД), подсистемы анализа защищенности (3.ПАЗ), подсистемы обнаружения и защиты от вторжений (4.ПЗВ), подсистемы защиты от вредоносных кодов (5.ПЗВК), подсистемы криптографической защиты (6.ПКЗИ), подсистемы контроля целостности (ПКЦ).

Результаты прогнозирования данных в каждом канале контроля качества с использованием полимодельного алгоритма регрессионного анализа приводятся на поле мониторинга в интервале времени от 13:10 (текущий момент времени) до 13:40, т.е. с упреждением на 30 минут, что весьма значительно с учетом высокой динамики процессов информационного противоборства [1], [3].

На поле мониторинга ИБ приведен фрагмент имитации угрозы (на момент времени 13:30) и невыполнения заданных требований (НТ) по ИБ (на момент времени 12:44) по значению агрегированного (сводного) показателя качества в канале контроля защищенности ИР «Соболь» с соответствующими рекомендациями (проектом управленческих решений), принятых офицером по ИБ соответственно в 12:32 и в 12:48. На 12:54 согласно режима имитации и принятого сценария моделирования в «СПРУ-ИБ» угроза и НТ по каналу «Соболь» ликвидирована за счет принятых мер.

На 13:18 зарегистрирована угроза, а на 13:26 НТ по каналу контроля «Страж», что привело к возникновению угрозы НТ на 13:30 по подсистеме ПМУБ в целом согласно результатам мониторинга.

Результаты и накопленный опыт проведения имитационного моделирования с использованием программного комплекса «СПРУ-ИБ» подтвердил правильность и перспективность принятых концептуальных, системных и технологических решений. Среди его конкурентных преимуществ – широкие и гибкие возможности мониторинга, прогнозирования и комплексного моделирования, а также тренажерной отработки различных сценариев управления информационными инцидентами и, прежде всего, в реальном масштабе времени, и по системным показателям качества АСзи.

Представленные варианты информационно-технологических решений задач мониторинга и управления защищенностью ИР ОМТИ демонстрируют, прежде всего, возможность их масштабирования, а это значит, что они могут рассматриваться в качестве типовых проектных решений со всеми вытекающими отсюда преимуществами. Прежде всего, простотой и малой

ресурсной затратностью при реализации. В сочетании с системным (целостным) характером решения задач мониторинга и управления ИР ОМТИ это дает принципиальное конкурентное преимущество, чем обуславливается возможность и необходимость первоочередного внедрения рассмотренных новых принципов и реализующих их информационных технологий мониторинга и управления в классе систем автоматизации управления защищенностью информационных ресурсов разнородных ОМТИ.

СПИСОК ЛИТЕРАТУРЫ

1. Сулакшин С.С. Когнитивное оружие – новое поколение информационного оружия – Вестник Академии военных наук, 2014, № 1 (46), с. 57 – 65.
2. Об утверждении технического регламента о безопасности объектов морского транспорта - Постановление Правительства РФ от 12 августа 2010 г. N 620
3. Савин Л.В. Сетецентрическая и сетевая война. Введение в концепцию. – М.: Евразийское движение, 2011.
4. Алексеев А.В. Технология и программный комплекс квалиметрической ранговой оценки качества сложных информационно-аналитических систем / Материалы IX Всероссийской научно-практической конференции МОРИНТЕХ-ПРАКТИК «Информационные технологии в судостроении–2008». – СПб., ОАО «Северные верфи»,19.06.2008, с.110-118.
5. Алексеев А.В., Орлов К.М. Информационно-аналитическое обеспечение современных специальных информационно-управляющих комплексов: состояние, проблемы и перспектив развития. Статья, сборник «Состояние, проблемы и перспективы разработки корабельных информационно-управляющих комплексов. / Сборник докладов научно-технической конференции. – М.: ОАО «Концерн «Моринформсистема-Агат», Москва, 2010, с.69-75.
6. Алексеев А.В. Методология синтеза системотехнических решений автоматизации процессов борьбы за живучесть судов повышенного риска /Актуальные проблемы морской энергетики: материалы третьей Всероссийской межотраслевой научно-технической конференции. – СПб.: Изд-во СПбГМТУ, 2014, с. 181 с.
7. Тюрин И.С., Алексеев А.В. Анализ технологии «10-STRIKE» для решения задачи мониторинга безопасности информационных ресурсов объектов морской техники и инфраструктуры – 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. – С.479-480.
8. Официальный сайт компании «10-Strike Software» (РФ, с 1998). - https://www.10-strike.com/rus/.
9. Официальный сайт компании «Symantec» (с 1995). - http://www.symantec.com/.
10. Волков В.И., Тычинин И.Ю., Алексеев А.В. Системные аспекты управления развитием современных критических объектов морской техники и морской инфраструктуры – 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. – С.447-448.
11. Федоров А.Е., Алексеев А.В. Развитие информационных технологий объектов морской техники и морской инфраструктуры – Там же, с. 484 - 485.
12. Тюрин И.С., Алексеев А.В. Оперативная и объективная оценка уровня информационной защищенности корпоративной сети – Там же, с. 477- 478.
13. Алексеев А.В., Ливанов И.В., Мусатенко Р.И. Информационная технология систем поддержки решений и управления, инвариантная к специфике задач объектов морской техники и инфраструктуры – Там же, с. 437- 438.
14. Алексеев А.В. Управление технической системой безопасности в промышленности / Системы безопасности. Журнал для руководителей и специалистов в области безопасности, 2004, № 6 (60), с. 68 - 73.

УДК 681.5.03

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ ТРЕНАЖЕРНОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ВМФ

Алексеев Сергей Алексеевич[1], Алексеева Елена Кирилловна[2]
[1]Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1
[2]Государственный университет морского и речного флота имени адмирала С.О. Макарова
198035, Санкт-Петербург, Россия, ул. Двинская, 5/7

Аннотация: В статье рассматривается постановка и решение задачи максимизации эффективности использования и минимизации стоимости технических средств обучения, входящих в состав учебно-материальной базы учебного заведения, для обеспечения тренажерной подготовки специалистов по управлению техническими средствами, с использованием математического аппарата линейного программирования и стандартного пакета прикладных программ.

Ключевые слова*: учебно-материальная база, технические средства обучения, тренажерная подготовка, эффективность, показатели качества, специалист, линейное программирование.*

ALGORITHMS FOR DETERMINING THE COMPOSITION OF THE TECHNICAL MEANS IN NAVAL TRAINING SIMULATOR

Sergey Alekseev[1], Elena Alexeeva Kirillovna[2]
[1]St. Petersburg University of the Ministry of Interior of Russia,
Petersburg, Russia, st. Pilot Pilyutov, d. 1
[2]Admiral Makarov State University of Maritime and Inland Shipping
St. Petersburg, Russia, st. Dvinskaya, 5/7

Abstract: This article describes fulfillment of the goal of effectiveness maximization and cost minimization of the technical means of training, which are the part of the material base of training center, for the purpose of

specialists simulator training, using mathematical methods of linear programming and standard package of applied programs.

Keywords: *material base, technical means of training, effectiveness, quality indicators, specialist, linear programming.*

В современной версии стандарта ИСО-9000 установлено, что, кроме системы управления качеством, в систему менеджмента качества должна входить система обеспечения. Исходя из этого положения следует, что технические объекты (ТО), составляющие в совокупности учебно-материальную базу (УМБ) обеспечения реализации мероприятий тренажерной подготовки (ТП), считать составной частью системы обеспечения качества ТП. В состав УМБ обеспечения ТП могут входить:

1) различные виды простых технических средств обучения, объединяющие технические устройства (аппаратуру) и дидактические средства обучения (носители учебной информации), которые с помощью технических средств обучения (ТСО) воспроизводятся;

2) тренажеры как один из классов ТСО, представляющие специализированные учебно-тренировочные устройства, которые предназначены для формирования умений и навыков, т.е. являются основными техническими объектами УМБ тренажерной подготовки;

3) тренажерно-обучающие системы (ТОС) объединяющие собственно тренажер и автоматизированную обучающую систему, что позволяет повысить эффективность процесса ТП.

Обоснованное включение в состав УМБ, обеспечивающей ТП, любых из перечисленных видов ТО должно опираться на выработку компромисса между двумя противоречивыми требованиями:

1) получение максимального эффекта от использования ТО в ходе ТП, т.е. выработку заданного уровня умений и навыков обучающихся;

2) сокращение расходов на закупку и внедрение ТО УМБ до минимума.

В основу достижения компромисса по удовлетворению указанных требований может быть положена взаимосвязь квалификационных требований (КТ), устанавливаемых в руководящих документах по ТП, и соответствующих ТО, обеспечивающих их удовлетворение. Наличие взаимосвязи должно характеризоваться уровнем выполнения *i-го* КТ с помощью *j-го* ТО, который может быть включен в состав УМБ обеспечения ТП, проводимой в рамках часов учебной программы ТП. Сами КТ должны быть проранжированы экспертами и каждому из них определен весовой коэффициент. Кроме того, должны быть известны затраты на закупку и внедрение в процесс ТП *j-го* ТО.

Исходя из сказанного, могут быть определены виды формул, которые в совокупности определяют модели процедур удовлетворения обоим требованиям. Эти формулы введены в работах по исследованию операций [1], [4], [5], [7], [9] и апробированы в вузах ВМФ [6], МЧС [8] и железнодорожных войск [2].

Пусть введена переменная

$$\rho_{ij} = \begin{cases} 1 \ \ при \ \ \beta_{ij} \geq \beta_i^{TP}; \\ 0 \ \ при \ \ \beta_{ij} < \beta_i^{TP}, \end{cases} \tag{1}$$

где: β_{ij} – уровень выполнения *i-го* КТ с помощью *j-го* типа ТО УМБ обеспечения ТП, $i = \overline{1, m}$, $j = \overline{1, n}$,

β_i^{TP} – требуемый уровень выполнения *i-го* КТ.

При этом каждое *i-е* КТ, $i = \overline{1, m}$, должно обеспечиваться хотя бы одним ТО, для которого $\rho_{ij}=1$. Необходимо ввести еще одну переменную

$$x_{ij} = \begin{cases} 1 \ \ если \ \ j-й \ вид \ ТО \ включен \ в \ УМБ \ для \ выполнения \ i-го \ КТ; \\ 0 \ \ в \ противном \ случае. \end{cases} \tag{2}$$

На переменные ρ_{ij} и x_j накладывается ограничение

$$\sum_{j=1}^{n} \rho_{ij} x_i \geq 1 . \tag{3}$$

Вводится переменная

$$y_{ij} = \begin{cases} 1 \ \ если \ \ j-й \ вид \ ТО \ используется \ при \ выполнении \ какого-либо \ КТ; \\ 0 \ \ в \ противном \ случае. \end{cases} \tag{4}$$

Очевидно, $y_j=1$, если в *j-м* столбце матрицы $\left\| x_{ij} \right\|_{[m\times n]}$ хоть один из элементов $x_{ij}=1$, т.е.

$$y_j = 1 - \prod_{i=1}^{m} \left(1 - x_{ij}\right). \tag{5}$$

В свою очередь стоимость ТО, определяемых матрицей $\left\| x_{ij} \right\|_{[m\times n]}$ может быть оценена по формуле

$$C = \sum_{j=1}^{n} \left[1 - \prod_{i=1}^{m} \left(1 - x_{ij}\right) \right] C_j \,, \tag{6}$$

где C_j – стоимость *j-го* ТО.

Если вводится ограничение, что расходы на закупку ТО УМБ обеспечения процесса ТП не должны превышать допустимую величину $C_{доп}$, то необходимо выполнить неравенство

$$C \le C_{доп} \,. \tag{7}$$

На основе введенных переменных и констант может быть построена модель удовлетворения первого требования – максимизация эффекта от использования ТО в ходе тренажерной подготовки, в виде прямой задачи линейного программирования, заданной в стандартной форме:

Целевая функция

$$W(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} \omega_i \rho_{ij} \beta_{ij} x_{ij} \to \max_{x_{ij}} \,, \tag{8}$$

где ω_i – весовой коэффициент *i-го* КТ, определенный экспертами исходя из содержания ТП.

Ограничения:

$$C \le C_{доп} \,; \tag{9}$$

$$\sum_{j=1}^{n} \rho_{ij} x_{ij} \ge 1 \,; \tag{10}$$

$$x_{ij} = \{0, 1\}, \;\; i = \overline{1, m}, \;\; j = \overline{1, n} \,. \tag{11}$$

Ограничения (9) и (10) в некотором роде противоречивы. Если их совместное выполнение невозможно, то задача (8) – (11) не имеет решения, т.е. ее область допустимых решений окажется пустой. В этом случае следует либо увеличить количество выделяемых средств $C_{доп}$, либо пересмотреть возможности выполнения КТ для тех ТО УМБ, для которых соотношение $\beta_{ij} \ge \beta_i^{TP}$ не выполняется, например, увеличения количества времени на отработку умений и навыков, входящих в КТ.

Модель удовлетворения второго требования – минимизация расходов на закупку и внедрение ТО, входящих в УМБ обеспечения ТП, можно представить в виде обратной задачи линейного программирования в стандартной форме:

Целевая функция

$$W(x) = \sum_{j=1}^{n} C_j x_j \to \min_{x_j} \,. \tag{12}$$

Ограничения:

$$\sum_{j=1}^{n} \rho_{ij} x_j \ge 1 \,; \tag{13}$$

$$x_j = \{0, 1\}, \;\; j = \overline{1, n} \,. \tag{14}$$

Для определения значения уровня реализации *i-го* КТ с помощью *j-го* ТО УМБ можно использовать следующие характеристики ТО [4]:

1. Результативность ТО, оцениваемая уровнем обученности (уровнем выработанных умений и навыков) в ходе ТП по эмпирической формуле

$$P_{ij}^{кон} = P_{ij}^{нач} + \left(1 - \gamma_{ij}\right)\left(1 - \xi^n\right), \tag{15}$$

где: $P_{ij}^{кон}$ – конечный уровень обученности, оцениваемый вероятностью того, что обучающийся способен выполнить *i-е* КТ с использованием *j-го* ТО в конце тренировочного цикла,

$P_{ij}^{нач}$ – начальный уровень обученности, оцениваемый вероятностью того, что обучающийся до конца данного тренировочного цикла имеет какие-то начальные умения и навыки,

$\gamma_{ij}\, S_{ij} / S_i$ – адекватность *i-го* ТО УМБ штатному образцу технического средства (ТС) по *j-му* КТ,

S_{ij} – число действий по управлению ТС, которые нужно отрабатывать на *j-м* ТО для удовлетворения *i-го* КТ,

S_i – число действий, которые необходимо освоить для *i-го* КТ на штатном образце ТС, $\gamma_{ij}=0,5 \ldots 0,9$,

$\xi_{ij} = 0,7 \ldots 0,8$ - доля восприятия учебной информации, по *i-му* КТ с использованием *j-го* ТО, при $n=1$,

n – число тренировок с использованием *j-го* ТО УМБ.

2. Экономическая целесообразность применения ТО

$$Q = \frac{L_{Т.О}}{\sum_{i=1}^{n} L_{Ш.Тi}}; \tag{16}$$

$$Q \le Q_{Л.Ф}, \tag{17}$$

где: $L_{Т.О}$ – стоимость ТО, $L_{Ш.Тi}$ – стоимость единицы штатной техники, которую заменяет ТО УМБ, $Q_{Л.Ф}$ – лимит финансирования.

3. Технологичность применения ТО определяется как отношение

$$T = \frac{T_{Т.О}}{T_{Ш.Т}} = \{0, 1\}, \tag{18}$$

где: $T_{Т.О}$ – количество технологических показателей ТО,

$T_{Ш.Т}$ – количество технологических показателей штатной техники.

4. Психолого-педагогичность применения ТО оценивается с помощью тестирования и опросов с учетом удовлетворения четырем основным требованиям:

1) умения и навыки, формируемые в ходе ТП с использованием конкретного ТО УМБ, должны соответствовать умениям и навыкам профессиональной деятельности по управлению ТС;

2) ТО не должен формировать умения и навыки, дающие отрицательный эффект при переходе к реальной деятельности по управлению ТС;

3) ТО должен позволять изменять условия реализации деятельности;

4) ТО должен регистрировать результаты ТП для последующего анализа руководителем обучения.

Обобщенная оценка психолого-педагогичности ТО УМБ определяется по формуле

$$D = \frac{D_{Т.О}^{+}}{D_{общ}} = \{0, 1\}, \tag{19}$$

где: $D_{Т.О}^{+}$ – число аспектов, оказывающих положительное воздействие с помощью ТО УМБ на обучающегося в ходе ТП,

$D_{общ}$ – общее число аспектов, которые необходимо оказывать на обучающегося в ходе ТП.

На основе перечисленных характеристик, определяющих качество ТО УМБ, обеспечивающего ТП, можно оценить одиночный ТО УМБ, решив задачу линейного программирования с целевой функцией вида

$$Z_j = k_1 P_j^{кон} + k_2 T_j + k_3 D_j, \tag{20}$$

и ограничением

$$Q_j\left(P_j^{кон}, T_j, D_j\right) \le Q_{Л.Ф}, \tag{21}$$

где k_1, k_2, k_3 – весовые коэффициенты, определяемые экспертами.

Последовательность реализации процедуры с помощью функции поиск решения Microsoft Excel:

1. До использования функции поиск решения как при максимизации эффективности, так и минимизации стоимости необходимо:

– сформировать путем экспертного опроса матрицу групповых оценок ТО УМБ,

– сформировать путем экспертного опроса матрицу оценок функций принадлежности ТО УМБ к расплывчатому множеству лучших образцов ТО УМБ,

– сформировать путем экспертного опроса матрицу групповых оценок важности ТО УМБ,

– сформировать путем экспертного опроса матрицу выполнения требований к ТО УМБ.

2. Ввести исходные данные в виде трех последних матриц и реализовать функцию поиск решения**.** При этом формируются:

1) для максимизации эффективности набора ТО УМБ:

– матрица выбора ТО УМБ,

– три матрицы условий выбора ТО УМБ;

2) для минимизации стоимости набора ТО УМБ:

– матрица выбора ТО УМБ,

– две матрицы условий выбора ТО УМБ.

3. На выходе функции поиск решения в общих случаях формируются оценки эффективности и стоимости набора ТО УМБ.

Постановка задачи минимальной стоимости требуемого для обеспечения ТП набора ТО УМБ имеет единственный вариант. Постановка задачи максимальной эффективности требуемого набора ТО УМБ в условиях финансовых ограничений является вариативной и зависит как от уровня финансовых ограничений, так и от значения функции принадлежности показателя (10), задающего нижнюю границу требований к ТО УМБ по их соответствию предъявляемым КТ.

В ходе ТП может возникнуть проблема необходимости модернизации УМБ, в ходе которой необходимо определить как образцы ТО, которые следует оставить в составе УМБ, так и новые образцы, которые следует ввести в состав УМБ. Процедура разработки минимального по стоимости и достаточного по эффективности плана модернизации УМБ, обеспечивающей ход ТП специалистов ВМФ, путем использования функции, например, поиск решения Microsoft Excel.

В качестве исходных данных используются предложенные экспертами значения функции принадлежности каждого из рассматриваемых ТО УМБ (входящих в базу и перспективных) к расплывчатому множеству лучших образцов, а также стоимости каждого. Решение задачи средствами Excel позволяет получить как план получения максимального по эффективности набора ТО УМБ без ограничения на стоимость, так и ряд планов, которые оцениваются с учетом условий лимита финансирования и показателей абсолютной и относительной эффективности использования варианта комплектования УМБ.

Оценка адекватности принятия решения по выбору плана модернизации УМБ может быть осуществлена на основе анализа отзывов о качестве практической подготовки выпускников, тренажерная подготовка которых по управлению ТС проводилась на разных по составу ТО УМБ.

При определении требуемого набора ТО УМБ для обеспечения процесса ТП может возникнуть задача: распределить ТО УМБ на n видов КТ таким образом, чтобы каждый ТО УМБ удовлетворял только одному КТ и чтобы при заданной результативности каждого ТО УМБ для каждого КТ суммарный эффект был максимальным.

Пусть β_{ij}, $i, j = \overline{1, n}$ – результативность *i-го* ТО УМБ при удовлетворении j-го КТ. Тогда сформулированная задача будет заключаться в таком выборе по одному элементу матрицы $\left\| \beta_{ij} \right\|$ из каждой строки и каждого столбца, чтобы из суммы $\beta_{1j_1} + \beta_{2j_2} + \cdots + \beta_{nj_n}$, $j_k \neq j_l$, при *k≠l* была максимальной.

Необходимо ввести переменную

$$x_{ij} = \begin{cases} 1, & \text{если } i-\text{й ТО УМБ удовлетворяет } j-\text{му КТ}; \\ 0 & \text{в противном случае.} \end{cases} \tag{22}$$

Тогда задача может быть сведена к следующей задаче линейного программирования, которая может быть решена путем использования функции поиск решения Microsoft Excel. При этом среди неотрицательных целочисленных решений системы *2n* уравнений

$$\begin{aligned} x_{i1} + x_{i2} + \cdots + x_{in} &= 1 \quad \left(i = \overline{1, n}\right), \\ x_{1j} + x_{2j} + \cdots + x_{nj} &= 1 \quad \left(j = \overline{1, n}\right), \end{aligned} \tag{23}$$

означающих, что каждый ТО УМБ обеспечивает удовлетворение одного КТ и каждое КТ обеспечивается одним ТО УМБ, необходимо найти то, которое максимизирует целевую функцию

$$W(x) = \sum_{i=1}^{n} \sum_{j=1}^{n} \beta_{ij} x_{ij} \to \max_{x_{ij}}, \tag{24}$$

означающую суммарную результативность всех выбранных ТО УМБ.

Эту же задачу можно решить сетевым методом. Вследствие специальной структуры сетевых задач для них разработано большое число эффективных алгоритмов, среди которых есть «венгерский алгоритм» [3]. Решение задачи может быть записано в виде двухмерного массива $X = \|x_{ij}\|, \ i = \overline{1, m}, \ j = \overline{1, m}$, где m – число ТО УМБ или КТ. Искомая переменная

$$x_{ij} = \begin{cases} 1, & \text{если } i-\text{й ТО УМБ назначен на } j-\text{е КТ}; \\ 0 & \text{в противном случае.} \end{cases} \tag{25}$$

Критерий эффективности решения задачи включает элементы матрицы стоимостей $\|C_{ij}\|$, где C_{ij} - затраты, связанные с назначением *i-го* ТО УМБ на *j-е* КТ. Для заданного значения *m* ТО УМБ и КТ существует *m!* допустимых решений, которые строятся путем выбора одного элемента в каждой строке матрицы $X = \|x_{ij}\|$ и ровно одного элемента в каждом столбце этой матрицы.

Требуется минимизировать целевую функцию

$$W(x) = \sum_{i=1}^{m} \sum_{j=1}^{m} C_{ij} x_{ij} \to \min_{x_{ij}}, \tag{26}$$

при ограничениях:

$\sum_{j=1}^{m} x_{ij} = 1$ для всех *i* (каждый ТО УМБ удовлетворяет одно КТ),

$\sum_{i=1}^{m} x_{ij} = 1$ для всех *j* (каждое КТ удовлетворяет один ТО УМБ).

Проведенные исследования, описываемые в статье, позволили сделать следующие выводы:

1. Установлено, что УМБ обеспечения ТП специалистов ВМФ должна входить в систему менеджмента качества ТП. При этом в состав ТО УМБ должны, как правило, входить простые ТСО, тренажеры и тренажерно-обучающие системы, представляющие совокупность тренажера и автоматизированной обучающей системы.
2. Комплектование УМБ различными ТО должно опираться на два противоречивых критерия: максимизации эффективности (результативности, оперативности и ресурсозатратности) и минимизации затрат на приобретение и внедрение новых ТО в УМБ. Компромисс должен находиться исходя из взаимосвязи КТ и степени удовлетворения их соответствующим набором ТО, входящих в состав УМБ.
3. Для постановки и решения задач максимизации эффективности и минимизации стоимости используется математический аппарат линейного программирования и стандартные пакеты прикладных программ.
4. Для автоматизированного решения задач комплектации УМБ обеспечения ТП специалистов ВМФ необходимо использовать, следующие четыре процедуры:
   1) процедуру решения задачи максимизации эффективности УМБ;
   2) процедуру решения задачи минимизации стоимости УМБ;
   3) процедуру разработки плана модернизации УМБ в связи с изменением состава и/или содержания КТ в части формирования требуемых умений и навыков по управлению ТС;
   4) процедуру выбора ТО УМБ для удовлетворения конкретных КТ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев С.А. Модели и процедуры автоматизированного определения требуемого набора технических средств обучения тренажерной подготовки специалистов // Научное обозрение. - 2012. – №2. – С. 172–81.
2. Алексеев С.А., Алексеева Е.К. Задачи квалиметрии прогноза и диагностики достигнутого качества тренажерной подготовки специалистов по судовождению // Журнал университета водных коммуникаций. - 2012. – №1. – С. 172 – 179.
3. Алексеев С.А. Процедура выбора степени автоматизации системы управления качеством тренажерной подготовки// Научное обозрение.- 2011.– №5. –С.88-97.
4. Алексеев С.А., Алексеева Е.К. Построение частных моделей управления качеством содержания и технологии тренажерной подготовки специалистов по судовождению // Журнал университета водных коммуникаций.- 2010. – №3. – С. 223–234.
5. Алексеев С.А. Модель организации и процесса функционирования социальной организационно-технической системы как корпоративной сети МЧС // Проблемы управления рисками в техносфере. – 2008. – №2. - С. 64 – 74.
6. Вентцель Е.С. Исследование операций: задачи, принципы, методология – 2-е изд. / Е.С. Вентцель. – М,: – Наука, 1988. - 206с.
7. Власов В.В. Совершенствование учебно-материальной базы подготовки специалистов ЖДВ: Автореферат … канд. техн. наук. – Петродворец: ВМИРЭ, 2007. – 22с. ДСП
8. Грешилов А.А. Прикладные задачи математического программирования: Учебное пособие / А.А. Грешилов. – М.: Логос, 2006. – 288с.
9. Жуков Г.П. Военно-экономический анализ и исследование операций / Г.П. Жуков, С.Ф. Викулов. – М.: Воениздат, 1987. – 145с.

УДК 658.58

НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ ТЕХНОЛОГИЙ ДИАГНОСТИКИ РОТОРНОГО ОБОРУДОВАНИЯ

Баркова Наталия Александровна, Грищенко Дмитрий Вячеславович,
Санкт-Петербургский государственный морской технический университет,
Санкт-Петербург, Россия, ул. Лоцманская, дом. 3,
e-mails: barkova@vast.su, tstf@mail.ru

Аннотация: Рассмотрены особенности развития диагностики роторного оборудования по вибрации и току с использованием многоканальных средств их измерения и анализа. Анализируются технологии экспертной и автоматической диагностики в задачах управления и обслуживания по фактическому состоянию, реализуемые с разной глубиной и скоростью диагностирования.

Ключевые слова: *анализ вибрации; вибродиагностика; диагностика по току; система диагностики; управление по состоянию.*

DIRECTIONS OF DEVELOPMENT OF INFORMATION-MEASURING METHODS FOR THE DIAGNOSIS OF ROTARY EQUIPMENT

Nataliya Barkova, Dmitriy Grishchenko,
St. Petersburg State Marine Technical University,
Russia, Lotsmanskaya Street 3, St. Petersburg,
e-mails: barkova@vast.su, tstf@mail.ru

Abstract: The peculiarities of developing the rotating machinery diagnostics, executed by multichannel devices for measuring and analyzing vibration signal and electric current, are discussed. The methods of expert and automatic diagnostics for solving the problems in machine condition monitoring and maintenance with estimation of defect severity and time, necessary for diagnostics, are analyzed.

Keywords: *vibration analysis; vibrodiagnostics; diagnosis using current; diagnostic system; condition-based control.*

Одними из важнейших направлений развития информационных технологий является контроль, диагностика и прогноз состояния работающих машин и оборудования, в том числе роторного, позволяющие решать задачи защиты от аварий и снижения затрат на поддержание оборудования в рабочем состоянии. Решаются эти задачи путем своевременного обнаружения и прогноза развития потенциально опасных дефектов, а также оперативного выявления ошибок управления объектами и оценки их последствий после устранения. Необходимая для их решения информация содержится в рабочих и вторичных процессах, анализ которых в процессе эксплуатации и является основой диагностики роторного оборудования.

Качество диагностики и прогноза определяется тремя основными факторами – требуемой скоростью принятия решения, объемом доступной диагностической информации и эффективностью используемых алгоритмов диагностирования. Скорость принятия решений – главное условие, разделяющее диагностику роторного оборудования на три основных направления. Это оперативная диагностика, результаты которой могут использоваться в системах управления оборудованием, разовая диагностика (диагностическое обследование), используемая для дефектации оборудования при обслуживании (ремонте) или для оценки качества выполненных работ, и профилактическая диагностика с долгосрочным прогнозом состояния, необходимая для перехода на обслуживание и ремонт оборудования по состоянию. В развитии каждого из указанных направлений можно выделить общие задачи, которые связаны, прежде всего, с увеличением объема используемой информации и применением современных цифровых технологий ее получения. Существует и большая группа частных задач, направленных на оптимизацию технологий использования ранее накопленной информации, минимизацию затрат на принятие решений и снижение степени участия экспертов в постановке конкретных диагнозов.

Наиболее информативными для диагностики процессами в роторном оборудовании является изменение давления рабочей среды (жидкость/газ) и электромагнитного поля в зазоре электрической машины. Задача непосредственного измерения переменных составляющих давления и электромагнитного поля в необходимых для диагностики точках контроля достаточно сложна, поэтому вместо прямых измерений часто контролируют информативные вторичные процессы – возбуждаемую переменными составляющими давления и электромагнитного поля вибрацию неподвижных узлов и наведенные переменным полем токи в обмотках электрической машины.

Поскольку в основных режимах работы роторное оборудование вращается с определенным периодом, основной путь выделения информативных параметров – спектральный анализ вибрации и тока. При этом количество независимых информативных параметров в спектре может исчисляться

десятками, и даже сотнями. В спектрах вибрации диагностическая информация содержится в величинах (абсолютных и относительных) и частотах гармонических составляющих, а также в спектральной плотности случайных составляющих. В спектрах тока такая информация, как правило, содержится в относительных (к основной силовой составляющей тока) величинах и в частотах гармонических составляющих, причем количество информативных составляющих в токе меньше, чем в вибрации.

Расширение используемой диагностической информации может вестись путем роста количества контролируемых сигналов и свойств объекта, к которым в первую очередь относятся температура и анализ смазки. Второй путь расширения используемой информации – усложнение алгоритмов анализа, в том числе совместный (взаимный) анализ вибрации и тока в разных точках контроля роторного оборудования. Для этого необходимо проводить синхронные измерения широкополосных сигналов в разных точках контроля.

Развитие цифровых систем диагностики идет по пути повышения качества многоканальных измерений и проведения параллельного и взаимного анализа всех сигналов, в том числе вибрации и тока, а также других штатно, используемых в системах управления и защиты роторного оборудования. Многоканальные средства синхронных измерений диагностических сигналов вибрации и тока требуются для всех трех направлений развития диагностики. Так, задача оперативной диагностики – как можно быстрее выдать диагноз с высокой степенью достоверности, чтобы управлять оборудованием в зависимости от получаемых результатов. И эту задачу надо решать, в том числе, на неустановившихся режимах вращения, так как, например, на пусковые режимы вращения приходится более половины отказов роторного оборудования. Естественно, что многоканальные непрерывные измерения диагностических сигналов с их параллельным анализом и накоплением «истории» т.е. результатов их анализа за большой промежуток времени при работе без дефектов, особенно на пусках – обязательное требование к создаваемым системам оперативной диагностики.

Задача разовой диагностики (диагностического обследования) – определить состояние оборудования без «истории» и за ограниченное время, на которое выделяется объект для проведения диагностики и/или наладки. Отсутствие «истории» измерений компенсируется возможностью организовать специальные режимы работы объекта, например, повторные пуски, скачкообразные изменения нагрузки и т.п. для получения дополнительной информации. Многоканальные средства измерения и записи сигналов при разовой диагностике, во-первых, сокращают затраты времени на диагностику, а, во-вторых, позволяют проводить глубокий офлайн анализ параллельно записываемых сигналов в переходных режимах работы оборудования. Следует отметить, что разовая диагностика делится на два направления – на стенде (входной и выходной контроль продукции), когда по данным диагностики большой группы одинаковых объектов можно создать групповой «образ» бездефектного объекта, и диагностика на месте, когда такой группы, как правило, нет. В первом случае после создания «образа» бездефектного объекта можно автоматизировать дальнейший процесс диагностики и отказаться от услуг эксперта. Во втором случае без участия эксперта с опытом диагностики конкретного вида оборудования не обойтись, и задачей такой диагностики становится обеспечение условий для повышения производительности работ, выполняемых экспертом. Важнейшим из таких условий является обеспечение совместного по всем точкам контроля онлайн анализа диагностических сигналов, как в переходных, так и в установившихся режимах работы оборудования.

Задача глубокой диагностики – обнаружить все характерные для конкретного вида роторного оборудования дефекты на ранней стадии развития, отслеживать и прогнозировать их развитие, т.е. осуществлять мониторинг дефектов. Одна часть дефектов роторного оборудования на ранней стадии развития хорошо проявляется в сигналах вибрации и/или тока в установившихся режимах его работы, другая часть – в динамических режимах с изменением частоты вращения или нагрузки, третья – при многомерных измерениях вибрации, позволяющих контролировать форму колебаний оборудования или существенно снижать уровень некоррелированных помех. Современные многоканальные средства измерения позволяют проводить предварительную запись сигналов вибрации и тока во всех точках контроля в установившихся и неустановившихся режимах работы для последующего офлайн анализа с применением алгоритмов разной сложности, в том числе и многомерного анализа, требующего сигналов большой длительности. А периодическое проведение многоканальных измерений в установившихся и неустановившихся режимах работы роторного оборудования с сохранением либо записанных отрезков сигналов, либо результатов их анализа позволит вести мониторинг всех дефектов и осуществлять долгосрочный прогноз безаварийной работы оборудования. По сохраненным данным, в случае аварийного выхода объекта из строя при быстром ухудшении состояния из-за ошибок управления, имеется возможность проведения экспертизы причин отказа.

Развитие оперативной диагностики. Основные ограничения на возможности оперативной диагностики роторного оборудования накладывает требование ограничения времени постановки диагноза до значений, достаточных для использования результатов диагностики в процессах управления. Естественно, что нижний предел на время постановки диагноза не должен отражаться на

его достоверности при появлении опасных дефектов. При скачкообразных ухудшениях состояния, чаще всего возникающих на его пусках или из-за ошибок управления, время на отключение роторного оборудования системами аварийной защиты определяется 2-3 оборотами ротора. За это время выполнить операции диагностирования невозможно, минимальная граница времени при сборе данных для оперативной диагностики составляет 8-10 оборотов ротора, а для достоверности диагноза его надо трижды подтверждать. Поэтому средства оперативной диагностики используются параллельно средствам аварийной защиты, и их задачей является предупреждение аварийной ситуации с определением ее причины для перевода объекта в безопасный режим работы или для вывода объекта в обслуживание (текущий ремонт) в штатном режиме.

Основных направлений развития средств оперативной диагностики, которые строятся в виде либо стационарных, либо стендовых систем – два. Первое – сокращение времени сбора диагностической информации до минимально возможного без снижения достоверности диагноза. Основной путь развития – совершенствование методов анализа сигналов ограниченной длительности. Второе – обеспечение раннего обнаружения ошибок управления с идентификацией вида ошибки. Основной путь – расширение количества объектов контроля, охваченной системой, так как ошибки управления обычно изменяют текущее состояние нескольких объектов, и расширение номенклатуры обнаруживаемых ошибок управления и их признаков.

Примером современной системы оперативной диагностики является СМД-4, разработанная специалистами ООО «Вибротехника». Это сетевая система, состоящая из работающих в сети Ethernet универсальных малогабаритных измерителей вибрации, тока и других сигналов и подключенного к той же сети компьютера с программой мониторинга и диагностики ОДА. Схема системы приведена на рисунке 1.

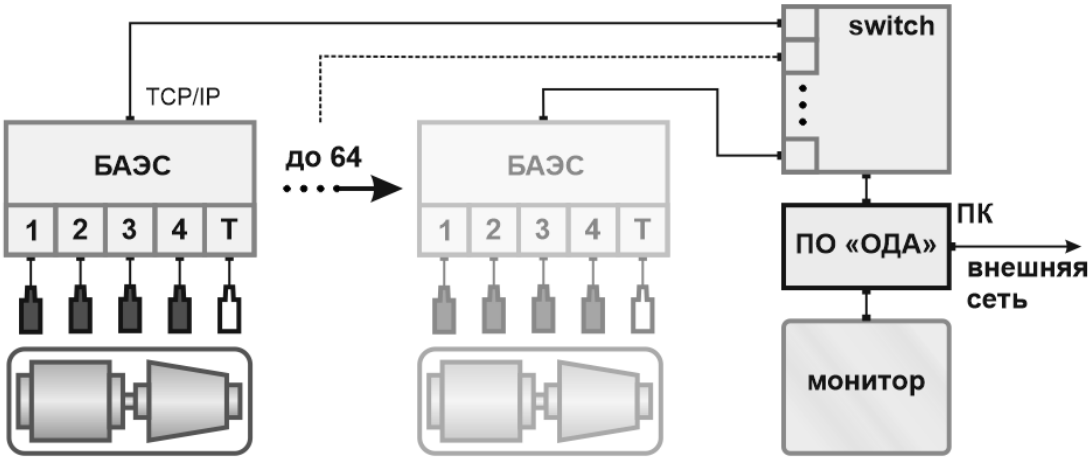


Рис.1. Структура многоканальной системы мониторинга и диагностики СМД-4.

Универсальный измеритель – это блок анализа электрических сигналов (БАЭС), к входам которого подключается группа измерительных преобразователей (датчиков). Задача БАЭС – непрерывный анализ поступающих на входы сигналов с выдачей результатов анализа в измерительную сеть. Количество подключаемых датчиков к каждому измерителю – до девяти, из них четыре датчика динамических сигналов вибрации или тока, четыре датчика медленно изменяющихся процессов (температуры, давления и т.п.) и один датчик оборотов ротора диагностируемой машины.

Программа мониторинга и оперативной диагностики ОДА получает результаты параллельного анализа сигналов со всех БАЭС из измерительной сети и проводит обработку входных данных с определением более 100 информативных параметров в каждой точке контроля. Совокупность всех контролируемых параметров вибрации и тока достаточно полно отражает состояние объекта мониторинга и позволяет обнаружить его опасное изменение из-за дефектов или ошибок управления в кратчайшее время, не превышающее пяти секунд, а также, при сохранении тенденций ухудшения состояния, позволяет оценить остаточный ресурс. Обнаружение и анализ тенденций изменения состояния после ликвидации ошибок обслуживания контролируемого оборудования или управления им в процессе эксплуатации позволяет оценить последствия этих ошибок.

Система рассчитана на мониторинг состояния и диагностику вращающегося оборудования с частотой вращения привода от 200 об/мин и выше. При этой частоте вращения диагностика выполняется за время, соответствующее 10 оборотам ротора, а с тройным подтверждением диагноза – за время, соответствующее 20 оборотам ротора. Для оборудования с передачами, снижающими частоту вращения выходного вала, на диагностику требуется дополнительное время. Конструктивная простота реализации СМД-4 позволяет использовать ее и в качестве переносной стендовой системы диагностики при обкатке оборудования после ремонта (монтажа) на месте для выявления скрытых дефектов, проявляющихся в первые часы работы.

Развитие разовой диагностики на основе диагностических обследований. Разовые диагностические обследования могут выполняться на месте эксплуатации после монтажа (наладки, обслуживания) роторного оборудования или на специальных стендах – при выходном контроле после изготовления (ремонта) или периодическом контроле состояния передвижных объектов диагностики. Накопленная «история» может использоваться для диагностики на месте, если она накоплена ранее, до решения о проведения обслуживания (текущего ремонта). В остальных случаях необходимую диагностическую информацию получают двумя способами – сравнением результатов текущих измерений диагностических параметров с данными таких же измерений группы аналогичных объектов (диагностика «по группе») или проведением расширенных диагностических обследований объекта на разных режимах работы, выполняемых по разработанным для конкретных типов объектов программам.

Диагностика «по группе» может проводиться в автоматическом режиме, для этого разрабатывается специальное диагностическое программное обеспечение, примером которого является пакет программ DREAM, выпускаемый Ассоциацией BACT. Но подобные системы не обеспечивают разового диагностирования несерийного роторного оборудования, не имеющего доступной для измерения вибрации группы аналогов, а именно такое оборудование чаще всего нуждается в персональной «доводке» технического и вибрационного состояния. Соответственно, такая доводка требует дополнительной диагностической информации, получаемой в процессе диагностического обследования, проводимого экспертами. Объем получаемой при информации можно увеличить несколькими способами, из которых основной – анализ вторичных процессов в динамических режимах работы объектов, в частности на пусках, в процессе прогрева после выхода на режим, при резких торможениях, скачках нагрузки и других тестовых воздействиях.

Для сокращения времени на диагностическое обследование необходимо минимизировать время на сложные виды анализа измеряемых в динамике вибрации и тока, и обеспечивать представление полученных данных в удобном для эксперта виде. Поэтому развитие технологий диагностических обследований идет в направлении увеличения количества параллельных каналов в средствах измерения диагностических сигналов и обеспечения их онлайн анализа. Важнейшим направлением становится еще и совместная по всем измерительным каналам онлайн обработка получаемых данных с предоставлением эксперту общей по каналам оценки вибрационного, а, при необходимости, и технического состояния.

Подобная многоканальная система, рассчитанная на параллельные измерения и онлайн анализ вибрации в большой группе (до 32) разнесенных на большие расстояния точках контроля разработана специалистами ООО «Вибротехника», рисунке 2. Главной особенностью этой системы является формирование объединенного по всем точкам контроля показателя со временем обновления в онлайн режиме – до 4 раз в секунду.

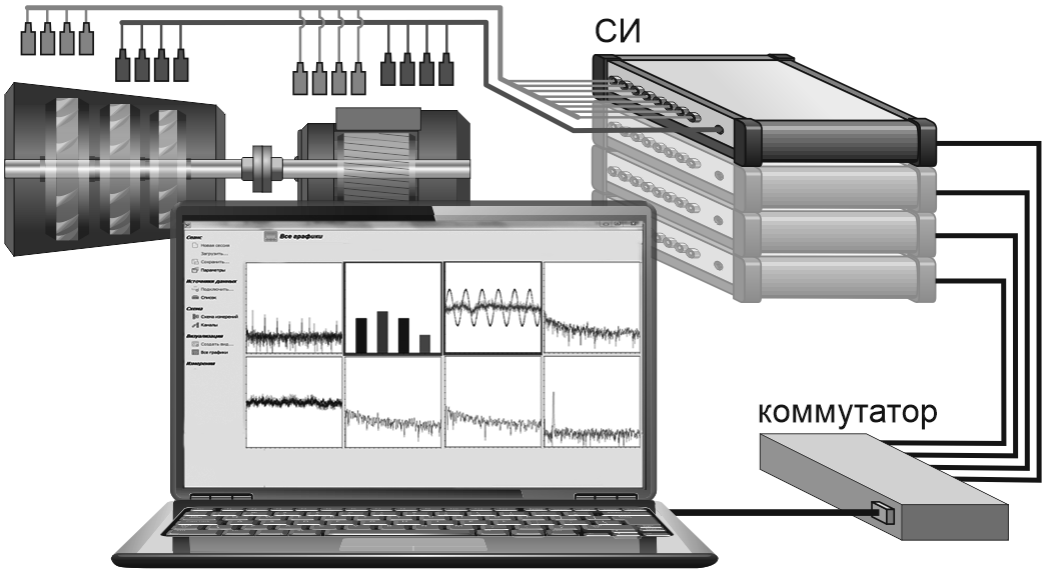


Рис. 2. Многоканальная система онлайн анализа сигналов с возможностью объединенной по каналам обработки данных.

Система рассчитана на параллельный анализ сигналов, снимаемых как с одного, так и с нескольких агрегатов, работающих на один технологический процесс, что дает возможность выявлять проблемы управления этим процессом.

Развитие превентивной диагностики. Превентивная диагностика основана на периодических измерениях диагностических сигналов во всех точках контроля каждого агрегата с обнаружением типовых дефектов в момент зарождения и контролем их развития во времени. Такая диагностика является основой перехода на обслуживание роторного оборудования по фактическому состоянию,

так как позволяет после регистрации момента перехода обнаруженных дефектов в развитое состояние начать подготовку к ремонту.

Наибольшее распространение получили переносные системы диагностики роторного оборудования по вибрации, которые используются в режиме разовой «групповой» автоматической диагностики (см. предыдущий раздел). Периодичность диагностики составляет 2–3 месяца, а после обнаружения дефектов и до момента вывода в ремонт интервалы сокращаются по мере развития наиболее сильного из обнаруженных дефектов, что позволяет отслеживать «историю» развития дефектов, прогнозируя момент достижения ими критической величины или скорости развития. Совершенствование такого рода систем идет по пути повышения достоверности обнаружения и идентификации дефектов, особенно на ранней стадии развития, для чего необходимо увеличивать объем используемой системой информации и, как следствие, количество независимых диагностических признаков.

Увеличение объема диагностической информации, производится за счет увеличения числа точек контроля, дополнительного измерения и анализа переходных процессов и пространственного анализа вибрации в установившихся и переходных режимах работы объекта.

Использование диагностических сигналов, измеряемых в неустановившихся режимах работы, хотя и усложняет их анализ, дает возможность охватить диагностикой еще и вращающееся оборудование многократного действия с коротким временем работы, в частности приводы станков, запорной арматуры и т.п. Особенность периодической диагностики такого оборудования – большинство видов анализа записываемых в переходном режиме работы оборудования сигналов переводится в офлайн режим.

В случае невозможности строить систему превентивной диагностики на основе построения «группового образа» бездефектного объекта с мониторингом и анализом «истории» развития дефектов приходится переходить на технологию мониторинга параметров состояния индивидуального объекта.

Эта технология основана на достаточно частых измерениях контролируемых в оборудовании процессов стационарно устанавливаемыми средствами измерения, т.е. стационарными «сборщиками» данных или системами диагностики. Поэтому и используется она, прежде всего, для диагностики наиболее ответственного и уникального роторного оборудования, не выпускаемого большими сериями.

Во многом эта технология совпадает с технологией оперативной диагностики, но есть и существенные отличия, определяемые тем, что не требуется непрерывность измерений, и нет ограничений на сложность и время обработки измеряемых сигналов, т.е. можно широко применять методы офлайн анализа предварительно записанных отрезков сигнала. Развитие этого направления, как и превентивной диагностики «по группе», идет по пути расширения количества признаков каждого дефекта за счет усложнения анализа сигналов во времени (переходные процессы) и в пространстве (по всем точкам контроля всей группы связанных системой диагностики объектов).

Таким образом, в развитии современных информационно – измерительных технологиях диагностики роторного оборудования по сигналам вибрации и по току приводных двигателей наметилась две основных тенденции.

Одна – объединение с технологиями управления объектами диагностики, при котором главной задачей является использование быстрых методов анализа в режиме онлайн.

Вторая – рост объема используемой для профилактической диагностики информации за счет усложнения методов офлайн анализа предварительно записанных сигналов.

Обе тенденции развития основаны на использовании многоканальных цифровых средств параллельного измерения диагностических сигналов с расширенными возможностями их быстрого онлайн и расширенного офлайн анализа.

К наиболее перспективным средствам диагностики можно отнести уже разработанные стационарные автоматические системы оперативной диагностики опасных дефектов, не требующие обслуживания и с возможностью автоматического накопления и передачи в удаленные службы диагностики информации для долгосрочного прогнозирования состояния и планирования обслуживания (ремонта).

СПИСОК ЛИТЕРАТУРЫ

1. Баркова Н.А. Введение в виброакустическую диагностику роторных машин и оборудования. – СПб: изд. центр СПбГМТУ, 2002, 156 с.
2. Неразрушающий контроль: Справочник: В 7т. Под общей редакцией В.В. Клюева. Т. 7: В 2 кн. Кн. 2: Ф.Я. Балицкий, А.В. Барков, Н.А. Баркова и др. Вибродиагностика. - М.: Машиностроение, 2005, 829 с.
3. Барков А.В., Баркова Н.А., Грищенко Д.В., Федорищев В.В. Система мониторинга вибрации с оперативной идентификацией обнаруживаемых изменений. Сборник докладов Всероссийской научно-практической конференции с международным участием «Защита от повышенного шума и вибрации». – СПб.: 2013, 743 с.
4. Барков А.В., Борисов А.А., Грищенко Д.В. Разработка многоканального online анализатора для исследования вибрации в широком диапазоне частот. Сборник докладов Всероссийской научно-практической конференции с международным участием «Защита от повышенного шума и вибрации». – СПб.. 2013, 743 с.

УДК 519.872.6

ФОРМИРОВАНИЕ ОПТИМАЛЬНОГО РАСПИСАНИЯ ДВИЖЕНИЯ СУДОВ ЧЕРЕЗ ШЛЮЗ ПО КРИТЕРИЮ МИНИМУМА ВРЕМЕНИ ПРОСТОЯ

Белоусов Игорь Владимирович,
Государственный университет морского и речного флота имени адмирала С.О. Макарова»,
Россия, Санкт-Петербург, ул. Двинская, д.5/7,
e-mail: ibel@bk.ru

Аннотация: Представлен алгоритм оптимального управления процессом шлюзования судов. Оптимальное решение задачи управления судопропуском ищется по критерию минимума простоя судов или грузов. Подробно изложено взаимодействие компьютерной системы шлюза с АИС шлюзуемых судов. Описан принцип формирования расписания шлюзований в зависимости от интенсивности потока судов. При составлении расписания шлюзований учитываются приоритеты судов. Проведено сравнение вариантов выбора расписаний шлюзования, определенных человеком и компьютером.

Ключевые слова: оптимизация; расписание; шлюзование; судопропуск; АИС

OPTIMUM SCHEDULING OF LOCKING SHIPS BY IDLENESS MINIMUM CRITERIA

Belousov Igor Vladimirovich,
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
e-mail: ibel@bk.ru

Abstract: Optimum control algorithm of locking ships is presented. Ship or cargo idleness minimum criteria are used for lock control and ship pass problem. Communications between computer system of the lock and AIS of the ships near the lock are described in details. Optimum scheduling concept is developed depending on ships traffic flow rate. Ships priorities take into account during locking ships scheduling. Computer and human locking ships schedules are compared.

Keywords: *optimization; schedule; ship locking process; ship pass; AIS*

Введение. Интенсивность движения по судоходным шлюзованным каналам имеет тенденцию к увеличению. Соответственно возрастает роль управления шлюзованием судов. Для решения проблем управления судоходством последнее время интенсивно привлекаются современные информационные технологии. К таким технологиям можно отнести автоматизированную систему управления технологическим процессом шлюзования (АСУ ТП) и автоматическую идентификационную систему (АИС). Системы автоматической идентификации судов являются навигационными системами, предназначенными для обмена навигационной информацией между судами и береговыми службами. Использование этих инновационных технологий позволяет повысить эффективность пропуска судов через шлюз.

Для автоматизации процесса шлюзования и пропуска судов через шлюз был разработан алгоритм автоматизированного управления.

Компьютерная система шлюза работает в тесном взаимодействии с АИС. Изначально АИС была создана с целью обеспечения безопасности судоходства. Определение местоположения судна осуществляется с помощью приемников ГНСС (ГЛОНАСС/GPS). В соответствии с требованиями международной конвенции SOLAS-74 (глава V «Безопасность мореплавания») все суда водоизмещением более 300 тонн должны быть оборудованы аппаратурой АИС класса А. Также в настоящее время на шлюзах Волго-Балтийского и Волго-Донского водного пути имеются береговые станции АИС. Эти станции соединены сетями передачи данных между собой и с пультами управления на шлюзах.

Таким образом, компьютерная система шлюза получает информацию АИС со всех судов, которые находятся в канале или на подходе к нему. Компьютерная система шлюза принимает следующие стандартные сообщения АИС [1]:

1. *Извещения о местонахождении* (тип сообщений 1,2,3):

– идентификатор морской подвижной службы (ИМПС) позволяющий однозначно идентифицировать судно;
– состояние судна (на ходу, на якоре, у причала);
– скорость относительно грунта;
– координаты судна;
– путь относительно грунта;
– истинный курс.

2. *Статические данные о судне* и сведения о рейсе (тип сообщения 5):

– название судна;
– тип судна и вид груза;
– пункт назначения;
– длина и ширина судна в метрах;
– расположение антенн ГНСС на судне;
– осадка судна в дециметрах.

Также компьютерная система шлюза принимает сообщения определенные стандартом для систем обнаружения и отслеживания судов на внутренних водных путях [2]. Если судно не передает такие сообщения, то используется информация из сообщений, указанных ранее. Компьютерная система шлюза принимает следующие сообщения:

1. Статические данные о судне внутреннего плавания и сведения о рейсе (тип сообщения 8, функциональный код 10):
– расширенный тип судна или состава;
– категория опасного груза;
– в грузу или порожнем;
– длина и ширина судна в дециметрах;
– осадка судна в сантиметрах.
2. Сообщение ETA к шлюзу/мосту/ терминалу (тип сообщения 6, функциональный код 21):
– предполагаемое время прибытия (ETA);
– надводный габарит судна.

На основании полученной информации компьютерная система определяет какие суда будут проходить через шлюз. При этом используется информация о пункте назначения судна, его курс, информация о состоянии судна.

Ожидаемое время прибытия судна берется из сообщения ETA. Данное сообщение является не обязательным и многие суда его не передают. В этом случае, время прибытия рассчитывается на основании текущего местоположения судна и его скорости. Если судно не передает скорость своего движения, то она рассчитывается по изменяющимся координатам судна.

При отсутствии необходимой информации вахтенный начальник шлюза может добавить ее вручную.

Для расстановки ожидающих шлюзование судов и судов в камере шлюза должны быть заданы:
– полезная длина и ширина камеры шлюза;
– длины и местоположения рейдов и причальных стенок.

Затем задается время шлюзования – это время от начала закрытия ворот до окончания открытия ворот противоположной головы шлюза. А также задается время швартовки судна.

Для каждого типа судна должны быть заданы:
– средняя скорость входа судна в шлюз с рейда;
– средняя скорость входа судна в шлюз от причальной стенки;
– средняя скорость выхода судна из шлюза до причальной стенки;
– средняя скорость выхода судна из шлюза до рейда.

На основании вышеуказанной информации компьютерная система составляет оптимальное расписание шлюзований судов. Оптимальное решение ищется по минимуму простоя судов или грузов.

Для формирования расписаний шлюзований было разработано несколько вариантов алгоритма:

1. Шлюзования судов в порядке их подхода к шлюзу. Не подошедшие к шлюзу суда не ожидаются. Данный алгоритм имеет линейную временную вычислительную сложность. Этот вариант использовался только для моделирования работы вахтенного начальника шлюза, с целью сравнения созданного им расписания с расписанием формируемым компьютерной системой.

2. Шлюзования судов в порядке их подхода к шлюзу. Максимально допустимое время ожидания судна рассчитывается в зависимости от интенсивности потоков судов. Данный алгоритм тоже имеет линейную временную вычислительную сложность и использовался только для моделирования работы вахтенного начальника шлюза. Для расчета максимально допустимого времени ожидания судна использовалась формула, найденная с использованием теории массового обслуживания [3]. Эта формула может быть использована вахтенным начальником на шлюзе, не оборудованном рассматриваемой здесь компьютерной системой.

3. Шлюзования судов в порядке их подхода к шлюзу. Время ожидания судна не ограниченно.

4. Шлюзования судов в порядке их подхода к шлюзу. Время ожидания судна не ограниченно. Можно не шлюзовать ожидающее судно.

5. Разрешается шлюзование судов в произвольном порядке с целью снижения времени простоя. Перестановка производится только для судов находящихся вблизи рейда или причальной стенки.

Все три последних варианта имеют, в худшем случае, экспоненциальную сложность. Однако в процессе работы алгоритма отбрасываются заведомо неоптимальные варианты. И в большинстве

практических случаев сложность решения данной задачи оказывается значительно меньше максимально возможной.

Была найдена среднестатистическая зависимость количества рассматриваемых в алгоритме судов от интенсивностей потоков судов, при заданной временной длительности работы алгоритма. Данная зависимость использовалась при моделировании работы алгоритма. Этой зависимостью можно воспользоваться и при составлении расписания на шлюзе. Но обычно на шлюзе требуется гарантировать составление расписания за заданное реальное время. Для этого задается не количество судов, участвующих в составлении расписания, а время работы алгоритма. Компьютерная система, в процессе вычислений, учитывает отбрасываемые варианты и корректирует количество рассматриваемых судов, с целью обеспечить заданное время работы.

Если в потоках судов присутствуют временные перерывы, то суда разбиваются на группы. Для каждой группы составляется расписание не зависимо от других групп.

При составлении расписания на шлюзе, расчет выполняется по алгоритмам с номерами 3, 4 и 5. Затем находится разница в суммарном времени простоя между алгоритмом с большим и меньшим номером. Если эта разница оказывается больше заданной, то расписание формируется по алгоритму с большим номером, в противном случае, расписание формируется по алгоритму с меньшим номером.

Формирование расписание шлюзуемых судов осуществляется в следующей последовательности. Вначале, в алгоритме учитываются только пассажирские суда и для них составляется расписание. Суда других типов при этом не рассматриваются. Затем составляется расписание для остальных судов. Суда, ожидающие у причальной стенки или на рейде, шлюзуются в порядке их приоритетов. Для этого задается уровень приоритета и максимально допустимое время простоя для каждого типа судна. Данная схема работы алгоритма полностью соответствует правилам пропуска судов и составов через шлюзы внутренних водных путей Российской Федерации [4].

Однако, в тех же правилах указано что при большом скоплении флота у границ допускается отступление от указанной выше очередности пропуска флота. Для этого при составлении расписания используется зависимость максимально допустимого времени простоя пассажирского судна от интенсивности потока судов. Эта зависимость задается в табличном виде. В строках таблицы указано допустимое время простоя при заданной интенсивности. При составлении расписания производится интерполяция по точкам, задающимся строками указанной таблицы. В элементарном случае, данная таблица содержит всего одну строку. В этой строке указывается, свыше какой интенсивности потока судов разрешается задерживать пассажирские суда, и на какое время их можно задерживать. Зависимость в этом случае представляет собой простейшую ступенчатую функцию.

Также есть возможность вместо зависимости от интенсивности потока судов, использовать зависимость от сэкономленного суммарного времени простоя судов.

Если интенсивность потока судов достаточно высока то сформированное расписание пассажирских судов корректируется на этапе составления расписания судов прочих типов, в соответствии с описанной выше зависимостью.

Рассчитанный порядок и планируемое время начала шлюзования судов выводится на экран пульта управления вахтенного начальника шлюза. Вахтенный начальник шлюза может изменить, при необходимости, автоматически сформированное расписание шлюзований. Для каждого судна он может указать либо точное время начала шлюзования этого судна, либо очередность его шлюзования. После этого компьютерная система произведет составление нового расписания с учетом этих изменений. Также, корректировка производится в случае, если судно не успевает подойти к назначенному времени начала шлюзования по техническим или иным причинам.

Рекомендуемое время прибытия передается на судно. Для этого ожидается сообщение ETA с судна. Если оно получено, то время прибытия передается в сообщении RTA (тип сообщения 6, функциональный код 22). В противном случае, время прибытия передается в виде текстового сообщения (тип сообщения 12) и ожидается подтверждение его приема. В случае отсутствия подтверждения приема сообщения судном на экран пульта управления вахтенного начальника шлюза выводится информация с просьбой передать рекомендуемое время прибытия по радиосвязи.

Решение о необходимости разведения моста (если такой имеется на шлюзе) принимается автоматизированной системой, на основании надводного габарита судна (из информации АИС) и уровня нижнего бьефа (из данных датчика уровня бьефа АСУ ТП шлюза). В любом случае судоводителю посылается текстовое сообщение «Высота под мостом». Таким образом, время разведения моста становится известно заранее и может быть выведено на информационное электронное табло моста для автомобилей, пересекающих канал.

АСУ ТП шлюза осуществляет автоматическое управление всеми светофорами шлюза на основании информации полученной с АИС и составленного расписания шлюзований. Дальний светофор шлюза автоматически переключается в зависимости от возможности пришвартоваться у причальной стенки. При наличии промежуточного светофора он автоматически переключается в зависимости от наличия встречного судна.

На компьютере вахтенного начальника шлюза осуществляется автоматическое ведение журнала судопропуска. Также, формируется база данных со статистической информацией. Эта информация включает в себя количество и время шлюзований, водоизмещение и типы шлюзованных судов, уровни бьефов. Имеются различные варианты анализа и вывода этой информации на экран.

Сформированное расписание шлюзований судов и собранная статистическая информация могут передаваться в компьютеры диспетчерской службы автоматически или по запросу.

Проводилось сравнение вариантов выбора расписаний шлюзования, определенных человеком и компьютером. Анализ работы человека показывает, что при низкой плотности потока судов он хорошо справляется с определением порядка следования судов через шлюз. Этот порядок практически всегда совпадает с оптимальным вариантом шлюзований, предлагаемым компьютером. При увеличении интенсивности потока судов увеличивается многообразие вариантов шлюзований. В этом случае человек не может перебрать большое количество вариантов шлюзований на большом промежутке времени и решения, принимаемые вахтенным начальником шлюза, не всегда совпадают с расписанием шлюзований, предлагаемом компьютерной системой.

Таким образом, разработка формальных методов принятия управленческих решений и их компьютерная реализация вместе с современными информационными системами позволяет более эффективно управлять шлюзом, а судоводителям планировать скорость движения и экономить топливо. Компьютерные технологии позволяют создать оптимальное расписание работы шлюзов, уменьшить время простоев судов в ожидании шлюзований.

СПИСОК ЛИТЕРАТУРЫ

1. Recommendation ITU-R M.1371-5. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band. – Geneva: ITU, 2014, 150c.
2. International Standard for Tracking and Tracing on Inland Waterways (VTT). Resolution No. 63. – New York, Geneva: United Nations, 2007, 57c.
3. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – М.: КомКнига, 2005, 400 с.
4. Приказ Министерства транспорта Российской Федерации (Минтранс России) от 3 марта 2014 г. №58 г. Москва "Об утверждении Правил пропуска судов через шлюзы внутренних водных путей" // Российская газета. – 2014, 22 авг. – №6462 (190) – с. 17.

УДК 621.1.07

ОПЫТ ОРГАНИЗАЦИИ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИИ КАЧЕСТВА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Бобрович Владимир Юрьевич, Антипов Василий Васильевич, Смольников Александр Васильевич,
Алексеев Анатолий Владимирович, Мусатенко Роман Иванович,
Институт автоматизации процессов борьбы за живучесть корабля, судна,
Россия, Санкт-Петербург, Ленинский пр., д. 101,
e-mail: iapbgks@bk.ru

Аннотация: В статье рассмотрен накопленный с 2012 г. опыт организации сертификации качества объектов морской техники по технологии РПС. В соответствии с новой концепцией, теорией и практикой добровольной ранговой партнерской сертификацией средств и систем, а в перспективе - аттестацией объектов информатизации в рамках партнерских объединений добросовестных производителей. Отличительными особенностями предлагаемой технологии сертификации являются квалиметрическая оценка качества изделий и услуг, а также её ранжирование с открытой публикацией соответствующих подтверждающих документов, в том числе, в сравнении с национальным и международным уровнем технологического развития. В рамках обобщенного опыта применительно к объектам морской техники показаны возможность реализации и апробированные технологии сравнительного анализа качества и повышения конкурентоспособности создаваемых изделий и услуг.

Ключевые слова: *конкуренция, сертификация соответствия и качества, ранжирование, управление развитием, интеллектуализация управления.*

THE EXPERIENCE OF ORGANIZING THE RANK OF PARTNER QUALITY CERTIFICATION MARINE FACILITIES

Vladimir Bobrovich, Vasily Antipov, Alexander Smolnikov, Anatoly Alekseev, Musatenko Roman,
Institute of automation of processes of the struggle for the survival of the ship, vessel,
Russia, St. Petersburg, Leninsky prospect, D. 101,
e-mail: iapbgks@bk.ru

Abstract: In the article accumulated from 2012 the experience of the organization of certification of quality marine facilities technology CPF. In accordance with the new concept, the theory and practice of voluntary rank partner certification tools and systems, and in the future - certification of objects of Informatization in the

framework of partnerships conscientious manufacturers. Distinctive features of the proposed technology certification are qualimetric assessment of the quality of products and services, as well as its rankings with open publication of the relevant supporting documents, including, in comparison with the national and international level of technological development. In the framework of a generalized practice in relation to marine facilities the possibility of realization and proven technologies comparative analysis of the quality and competitiveness of created products and services.

Keywords: *competition, compliance certification and quality, ranking, development management, intelligent management.*

Введение. 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 [1], [2].

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 [3], [4].

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 [1], [2], [3], [4].

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 изложены в [1], [2]. Прежде всего, это актуально для объектов информатизации, как наиболее востребованных в условиях интенсивного развития современных технологий и систем автоматизации.

К настоящему времени в соответствии с концепцией РПС в Некоммерческом партнерстве «Институт автоматизации процессов борьбы за живучесть корабля, судна» накоплен определенный положительный опыт, который, по нашему мнению, может быть полезен читателям специалистам.

Практическое решение проблемы повышения качества создаваемых АС ОМТ и их технологического развития на основе реализации концепции РПС, по нашему мнению, становится одним из наиболее доступных, реальных и системно целесообразных путей обеспечения конкурентоспособности АС ОМТ, минимизации потребительского риска при их использовании и развитии.

В основу РПС в условиях действия Федерального закона «О техническом регулировании» и национальной концепции добровольной сертификации положены следующие принципы РПС [5]:

– некоммерческого проведения сертификации изделий и услуг, формирования открытых баз данных и знаний по конкурентной способности сертифицированных средств;

– проведения квалиметрической независимой (объективной) и анонимной оценки качества изделий и услуг (количественного измерения качества) в рамках добровольных партнерских объединений добросовестных производителей с последующим ранжированием оценок качества и методически «прозрачным» определением уровня конкурентной способности;

– приоритетного использования технологий автоматической обработки результатов экспертного оценивания, независимой от негативного проявления субъективных (человеческих) факторов;

– открытости и прозрачности экспертного оценивания и документирования процедур РПС.

Другими отличительными признаками концепции РПС в сравнении с традиционными принципами сертификации соответствия изделий и услуг требованиям стандартов, регламентов и договоров являются:

– открытая публикация (прозрачность) соответствующих документов проведения сертификационных испытаний и фактически достигаемого при этом уровня качества;

– квалиметрическая оценка и публикация уровней конкурентной способности сертифицируемых изделий и услуг, в том числе, в сравнении с национальным и международным уровнями их технологического развития (сегодня этого практически нет);

– публикация соответствующих реестров сертифицированных средств и услуг с оценками достигаемых при этом уровней качества и конкурентной способности.

Таким образом, актуальность РПС в отличие от действующей системы сертификации (оценки соответствия требованиям стандартов, регламентов и договоров без оценок валидности изделий и услуг, то есть, количественной оценки степени достижения ими целей по предназначению) обусловлена: необходимостью перехода к квалиметрической (количественной) оценке и подтверждению соответствия продуктов и услуг (сертификации) достигаемому уровню качества и, как следствие, к оценке их конкурентной способности и преимуществ, в том числе, ранжированию полученных оценок в сравнении с национальным и международным (мировым) уровнем технологического развития.

Рассмотрим конкретный вариант реализации концепции РПС ЭТС ОМТ в судовых системах автоматизации, а также приведем достигаемые при этом преимущества и возможности обеспечения и повышения конкурентной способности создаваемых средств и систем автоматизации.

Среди преимуществ концепции РПС систем автоматизации ОМТ применительно к системам комплексной судовой автоматизации, например, класса подсистем информационной поддержки судоводителей (СИП) [2], [4], [5], следует выделить:

– прогрессивное саморазвитие и саморегулирование РПС (независимой и добровольной) за счет обеспечения условий равной конкуренции для участников некоммерческих классификационных партнерств (НП), формирования единых и достаточно простых условий и регламентов сертификации, а также существенно меньшего уровня стоимости РПС;

– квалиметрическое обеспечение оценивания конкурентоспособности изделий и услуг с «естественным» регулированием рынка и обеспечением адекватной защищенности потребителей;

– саморегулирование ценообразования объектов РПС и в целом ОМТ, обоснованного уровнем достигаемого качества за счет информационной прозрачности для Потребителя (Заказчика) фактических значений уровня качества АС и их конкурентной способности;

– ускорение технологического развития объектов РПС за счет качественно нового уровня взаимного партнерского обмена технологической информацией и тем самым естественного мотивирования наращивания уровня качества изделий и услуг, конкурентной способности при контролируемом уровне информационного риска для членов НП.

В качестве методологической базы конкурентного сравнения объектов сертификации и аттестации с учетом [1] ,[2], [3] принят переход от подтверждения соответствия требованиям стандартов, регламентов и договоров (как это принято при традиционной системе сертификации СА и в целом ЭТС, аттестации ОМТ) непосредственно к квалиметрической оценке (измерению) достигаемого уровня качества. При этом оценка качества производится с использованием комплекса как частных (ЧПК), так и групповых (ГПК, отражают соответствующие свойства), а также сводного (агрегированного) показателей качества (СПК) изделия или услуги. Именно это позволяет непосредственно переходить к сравнительной количественной оценке конкурентной способности и анализу конкурентных преимуществ разрабатываемых, используемых средств, систем и объектов автоматизации.

В свою очередь, сравнительная количественная оценка позволит совершенствовать сами процессы проектирования и выходить на высокие конкурентные уровни создаваемой продукции и предоставляемых услуг как на внутреннем, так и на внешнем рынке.

Важным методологическим вопросом взаимодействия членов НП при РПС является использование единых согласованных математических моделей сравнительной оценки качества оцениваемых технологических решений АС и средств её реализации. Это обеспечивает, с одной стороны, возможность методически прозрачной ранговой сертификации с квалиметрической оценкой достигаемого уровня качества и конкурентной способности средств, а, с другой стороны, верификацию и совершенствование разрабатываемых научно-методических аппаратов, их практическое и ускоренное внедрение и развитие. В том числе, в сравнении с корпоративными, национальном и международным (мировым) уровнем развития (в рамках альтернативных вариантов из состава непрерывно актуализируемой их базы данных и знаний).

Базовые положения подобной математической модели и методологии применительно к РПС могут быть заимствованы из результатов [1], [2], [3], [4], [5], прошедших достаточную апробацию и подтвердивших свою инвариантность к специфике целого ряда практических задач.

Ключевыми процедурами, методами и алгоритмами количественного анализа современных сложных по архитектуре и функциональным возможностям АС ОМТ могут быть названы три модели: обеспечения инвариантности используемых ЧПК к специфике каналов измерения и контроля качества (модель инвариантного канала контроля ЧПК); обеспечения интегрированной оценки качества ЭТС (модель агрегирования показателей качества); обеспечения классификации состояний канала контроля качества (модель классификации состояний канала).

1. Математическая модель инвариантного канала контроля ЧПК при измерении любого из организационно-технических параметров АС ОМТ (например, уровня давления, температуры, объема, стоимости устройств, уровня сертификации, степени выполнения регламентных работ и т.п.) в обобщенном виде может быть представлена следующим образом:

$$q_n^H = \{\frac{[q_n - Min(q_n)]^h \times [Max(q_n) - q_n]^{1-h}}{Max(q_n) - Min(q_n)}\}^P, \quad (1)$$

где:

q_n^H – нормированное по алгоритму (1) значение ЧПК для измеряемого параметра q_n с номером n;

P – степень нелинейности шкалы оценок, равная $P = 1$ для линейных шкал и определяемая, в общем случае, по данным статистического анализа (при их отсутствии принимается значение $P = 1$);

$h = 1$ – позитивный характер связи измеряемого параметра с качеством ЭТС (например, прочность корпуса судна; надежность АС, дальность действия локатора, обобщенный уровень качества ЭТС по данным сертификации, комфортность принятия решений, уровень дизайна и т.п.);

$h = 0$ – негативный характер связи измеряемого параметра с качеством ЭТС (например, стоимость изделия, массогабаритные характеристики устройства, длительность восстановления, степень негативного влияния субъективных (человеческих) факторов, уровень риска (любого рода), длительность цикла обоснования и принятия управленческого решения и т.п.);

$Min(q_n), Max(q_n)$ – минимальное и максимальное значения диапазона изменения оценок ЧПК q_n при функционировании АС ОМТ, определяемые, например, границами шкал приборов и т.п.

2. Математическая модель агрегирования показателей качества при оценке интегрированной оценки качества ЭТС при измерении комплекса организационно-технических параметров АС ОМТ по частным показателям качества (ЧПК) и их агрегирования в групповые показатели качества (ГПК, характеризуют различные свойства АС в составе ОМТ), а также агрегирования ГПК в модельные сводные показатели качества (МПК, определяются спецификой соответствующих моделей оценивания) и интегрированный СПК (характеризуют АС в целом), в обобщенном виде может быть представлена в виде, так называемого, гармонического алгоритма:

$$Q_n^{\Gamma} = \left\langle \prod_{n=1}^{N} q_n^{\alpha_n} \times \sum_{n=1}^{N} (\alpha_n \times q_n) \right\rangle^{0,5} \quad (2)$$

Отличительным преимуществом гармонического алгоритма свертки ЧПК в ГПК, а также ГПК в МПК и МПК в СПК, следует считать промежуточное (компромиссное) значение получаемых оценок СПК в сравнении с известными аддитивным (оптимистическим) и мультипликативным (пессимистическим) алгоритмами свертки. Это имеет особое значение для критических систем, в том числе, ОМТ, при показателях ЧПК, ГПК и МПК в области малых значений, так как обеспечивает минимизацию погрешностей оценивания СПК.

3. Математическая модель классификации состояний инвариантного канала контроля качества при измерении любого из организационно-технических параметров АС ОМТ (например, «соответствует заданным требованиям», «не соответствует заданным требованиям» и т.п.) в обобщенном виде подробно представлена в [5].

Применительно к названным выше задачам СИП обеспечения борьбы за живучесть судна состояние S_i инвариантного канала ЧПК $q(t)$ в соответствии с алгоритмом (2) и пороговыми уровнями q_{a1}, q_{a2}, … классифицируется по поддиапазонам значений ЧПК следующим образом: НС – нормальное состояние (работа по штатному); У1, У2 – угроза аварийной ситуации (аварии) по верхнему (1) и нижнему (2) порогам; А1, А2 – авариная ситуация по соответствующим порогам (АС); УЧ – угроза чрезвычайной ситуации по нижнему порогу; ЧС – чрезвычайная ситуация.

Аналогичным образом состояние инвариантных каналов контроля качества АС ОМТ классифицируется для групповых (ГПК), модельных (МПК) и сводного (СПК) показателей качества.

Практика реализации концепции РПС. К настоящему времени в ходе решения ряда практических задач накоплен определённый опыт и отработан ряд практических вопросов реализации излагаемой концепции и технологии РПС систем автоматизации ОМТ в процессе:

– формирования квалиметрической базы данных и знаний (КБДЗ) альтернативных технологических решений (ТР, включая патенты, изобретения, полезные модели, описания ТР по данным НИР и ОКР, статьи и т.п.) в классе систем информационной поддержки борьбы за живучесть корабля, судна (более 200 альтернативных технологических решений) [3], [4], [5];

– экспертного оценивания альтернативных ТР с использованием специально разработанных программных комплексов и методик оценивания «КРОПУР», «СППР ЭО», «БДЗ-БЖ», «МКО», «МКО-И» [4], [5]. Основные фрагменты технологии экспертного оценивания ТР с использованием программного комплекса АСППР ЭО ТР «МКО-И» (версия «МКО-БЖКС») приведены на рисунке 1;

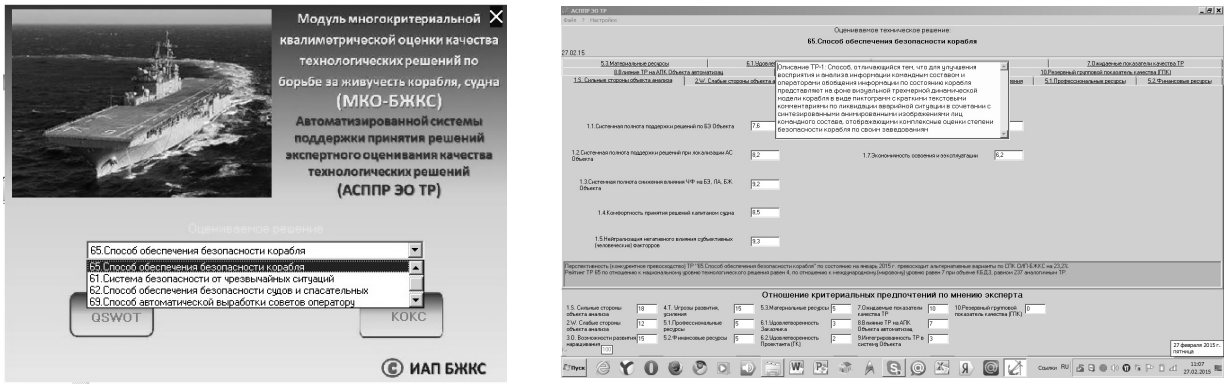


Рис. 1. Основные фрагменты технологии обеспечения экспертного оценивания СИП-БЖКС при использовании АСППР ЭО ТР «МКО-И»: выбор ТР; экспертная оценка ТР «65.Способ обеспечения…»

– автоматического формирования при реализации РПС комплекта документов: Заявителя (заявки на РПС в комплекте); Коллегиального сертификационного органа (КСО: решений о составе Партнерских экспертных советов (ПЭС) о возможности выдачи сертификата качества, сертификата качества ЭТС, реестра сертифицированных средств и т.п.); Центра РПС (ЦРПС: программ и методик, протоколов, акта проведения сертификационных испытаний и других); ПЭС (протоколов экспертного оценивания, автоматической оценки СПК, формирования и актуализации фонда электронного документооборота, квалиметрической базы данных и знаний (КБДЗ) по номенклатуре ПЭС и других);

– практической отработки регламентов проведения заседаний ПЭС, а также проведения публичных групповых экспертиз качества ЭТС, открытых заседаний ПЭС и других;

– открытой публикации материалов проведения РПС и публичного обсуждения концепции, технологии и практики квалиметрического сравнения технологических решений и оценки и конкурентной способности в реальных условиях анализа сложных ЭТС, в том числе класса СИП.

Так в апреле 2014 г. весьма успешно была проведена РПС в рамках Некоммерческого партнёрства «Институт автоматизации процессов борьбы за живучесть корабля, судна (ИАП БЖКС)». Экспертиза заявленных ТР была проведена в специальном формате сертификационных испытаний ЦРПС на открытом заседании Партнерского экспертного совета по рассмотрению результатов оценки конкурентной способности технологических решений класса «Системы информационной поддержки решений по управлению сложными эрготехническими системами повышенного риска».

При этом заявители представляли свои предлагаемые ТР в форме как заявочного комплекта документации, так и обязательных 10-минутных презентаций ТР с обоснованием заявляемого уровня конкурентной способности в безличной (анонимной) форме. Далее следовали индивидуальная (независимый, анонимная) экспертиза каждого ТР с использованием специально разработанных программных комплексов в защищенном исполнении и коллегиальное утверждение автоматически подготовленных протоколов и проекта решения Партнерского экспертного совета. Наконец, результаты сертификации качества ТР и оценки их конкурентной способности были публично оглашены и одобрены в рамках проводимого ИАП БЖКС цикла научно-практических семинаров.

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 (рис. 2).

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 [4], [5].

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.

СИСТЕМА ДОБРОВОЛЬНОЙ ПАРТНЁРСКОЙ РАНГОВОЙ СЕРТИФИКАЦИИ ПРОДУКЦИИ И АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Некоммерческое партнёрство «ИНСТИТУТ АВТОМАТИЗАЦИИ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА»

Свидетельство государственной регистрации № 1127800009039

ПАРТНЁРСКИЙ СЕРТИФИКАЦИОННЫЙ ЦЕНТР

СЕРТИФИКАТ КАЧЕСТВА

№ СК.0002 05.12.2013

ВЫДАН: ОАО «СПИК СЗМА» (199155, Россия, г. Санкт-Петербург, пер. Каховского, д. 10)

Настоящий Сертификат качества удостоверяет, что ПРОГРАММНЫЙ КОМПЛЕКС «АРБИТР», аттестационный паспорт № 222 от 21 февраля 2007 г., Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) со сроком аттестации на 10 лет, с числом уровней декомпозиции – 2, числом вершин основного суперграфа – до 400, числом вершин подграфов – до 100, с автоматическим построением логических и вероятностных функций показателей надежности, стойкости, живучести, безопасности и технического риска систем, с реализацией немонотонных систем (полной группы алгебры логики), циклических (мостиковых) связей, четырех законов распределения работного времени, статического и временного, вероятностного, детерминированного и сетевого режимов моделирования,

автор - Можаев Александр Сергеевич (RU),

соответствует уровню качества Q = 9,67, что по состоянию на 1.12.2013 соответствует рейтингу R = 1 по отношению к мировому уровню технологического развития автоматизированных систем поддержки принятия решений при проектном обосновании надежности, живучести и устойчивости сложных организационно-технических систем, включая объекты морской техники и морской инфраструктуры при объеме базы альтернативных вариантов систем поддержки принятия решений N = 12.

Исполнительный директор НП «ИАП БЖКС» А.В. Алексеев

Руководитель Партнерского сертификационного центра Р.И. Мусатенко

Зарегистрировано в Едином реестре ПСЦ за № RM002 от 05.12.2013 г.

СИСТЕМА ДОБРОВОЛЬНОЙ ПАРТНЁРСКОЙ РАНГОВОЙ СЕРТИФИКАЦИИ ПРОДУКЦИИ И АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Некоммерческое партнёрство «ИНСТИТУТ АВТОМАТИЗАЦИИ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА»

Свидетельство государственной регистрации № 1127800009039

ПАРТНЁРСКИЙ СЕРТИФИКАЦИОННЫЙ ЦЕНТР

СЕРТИФИКАТ КАЧЕСТВА

№ СК.0003 17.04.2014

ВЫДАН: ОАО «Концерн «НПО «Аврора» (194021, Россия, г. Санкт-Петербург, ул. Карбышева, д. 15)

Настоящий Сертификат качества удостоверяет, что «Технология и программные комплексы задач информационной поддержки управления техническими средствами при нормальной эксплуатации и при борьбе за живучесть корабля (ТПК ИП ТС БЖК)», регистрационный № ТР-175 от 2 апреля 2014 г. Открытого конкурса «КСТР-2014: Конкурентно способные технологические решения в классе средств информационной поддержки решений по управлению эрготехническими системами повышенного риска»,

авторы - коллектив НИУ-2 ОАО «Концерн «НПО «Аврора»,

соответствует уровню качества Q = 6,84 при коэффициенте вариации оценок 13,7% и индексе квалификации Экспертного совета 52,9%, что по состоянию на 17.04.2014 соответствует рейтингу Rн = 1 по отношению к национальному уровню технологического развития систем названного класса при объеме базы альтернативных вариантов систем поддержки принятия решений N = 178.

Исполнительный директор НП «ИАП БЖКС» А.В. Алексеев

Руководитель Партнерского сертификационного центра Р.И. Мусатенко

Зарегистрировано в Едином реестре ПСЦ за № RH005 от 17.04.2013 г.

СИСТЕМА ДОБРОВОЛЬНОЙ ПАРТНЁРСКОЙ РАНГОВОЙ СЕРТИФИКАЦИИ ПРОДУКЦИИ И АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Некоммерческое партнёрство «ИНСТИТУТ АВТОМАТИЗАЦИИ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА»

Свидетельство государственной регистрации № 1127800009039

ПАРТНЁРСКИЙ СЕРТИФИКАЦИОННЫЙ ЦЕНТР

СЕРТИФИКАТ КАЧЕСТВА

№ СК.0005 17.04.2014

ВЫДАН: ФГБУН «Институт проблем управления им. В.А.Трапезникова Российской академии наук» (117997, Россия, г. Москва, ул. Профсоюзная, д. 65)

Настоящий Сертификат качества удостоверяет, что «Проектирование СИПР для морских подвижных объектов на основе методов теории интеллектуального управления и полномасштабного имитационного моделирования», регистрационный № ТР-176 от 7 апреля 2014 г. Открытого конкурса «КСТР-2014: Конкурентно способные технологические решения в классе средств информационной поддержки решений по управлению эрготехническими системами повышенного риска»,

авторы - Данилова С. К., Борисов В. Г., Тарасов Н. Н., Аминев Б. Д., Кусков А. М., Кусков И. М., Лапицкий А. Д., Миненок А. Е., Хримпач К. М.

соответствует уровню качества Q = 5,75 при коэффициенте вариации оценок 13,7% и индексе квалификации Экспертного совета 52,9, что по состоянию на 17.04.2014 соответствует рейтингу Rн = 3 по отношению к национальному уровню технологического развития систем названного класса при объеме базы альтернативных вариантов систем поддержки принятия решений N = 173.

Исполнительный директор НП «ИАП БЖКС» А.В. Алексеев

Руководитель Партнерского сертификационного центра Р.И. Мусатенко

Зарегистрировано в Едином реестре ПСЦ за № RH005 от 17.04.2013 г.

Рис. 2. Сертификаты качества, выданные ОАО «СПИК СЗМА» (рейтинг Rм=1 по отношению к мировому уровню), ОАО «Концерн «НПО «Аврора» (рейтинг Rн=1 по отношению к национальному уровню, в классе средств СИП), ФГБУН «Институт проблем управления им. В.А.Трапезникова РАН» (Rн=3, в классе средств СИП)

Заключение. 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. 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.

СПИСОК ЛИТЕРАТУРЫ

1. Смольников А.В, Алексеев А.В., Антипов В.В., Бобрович В.Ю. Ранговая сертификация современных эрготехнических систем, как реальный способ повышения конкурентоспособности объектов морской техники и морской инфраструктуры – Морской Вестник, 2013, № 2 (14).

2. Смольников А.В., Алексеев А.В., Антипов В.В., Бобрович В.Ю. Пути повышения конкурентной способности объектов морской техники и морских транспортных систем на основе создания баз данных и знаний технологических решений и их ранговой сертификации / Вторая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем» ИКМ МТМТС 2013. Санкт-Петербург, 03-04 июля 2013 года. - ИКМ МТМТС 2013 – SCM MEMTS 2013, с. 109-114.
3. Алексеев А.В. Сертификация систем обработки информации. – СПб.: СПбГМТУ, 2010. – 159 с.
4. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор». Спб., 7-9.10.2014 – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С. 29-34.
5. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Ранговая партнерская сертификация качества: концепция, теория, практика / Региональная конференция (РИ-2014). XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Труды конференции. \ СПОИСУ. – СПб, 2014 (в печати).

УДК 57.087.1

БИОМЕТРИЧЕСКИЕ МЕТОДЫ АУТЕНТИФИКАЦИИ: НАСТОЯЩЕЕ И БУДУЩЕЕ

Бориев З.В., Соколов С.С.,
Государственный университет морского и речного флота имени адмирала С.О. Макарова»,
Россия, Санкт-Петербург, ул. Двинская 5/7, тел. (812) 748-97-20
e-mail: za_mir_b@mail.ru, sssokolov@mail.ru

Аннотация. В данной статье рассмотрены возможности применения биометрических информационных технологий для аутентификации пользователей в информационных системах. Проанализированы биометрические методы и системы идентификации пользователя. Даются рекомендации по использованию тех или иных систем в зависимости от специфики решаемых задач.

Ключевые слова: *биометрия, аутентификация; биометрические параметры; вейвлет-анализ.*

BIOMETRIC METHODS OF AUTHENTICATION: PRESENT AND FUTURE

Z.V. Boriev, graduate student, S.S. Sokolov, PhD,
Admiral Makarov State University of Maritime and Inland Shipping
Dvinskaya st. 5/7, St. Petersburg, Russia, 198035, tel. (812) 748-97-20
e-mail: za_mir_b@mail.ru, sssokolov@mail.ru

Abstract. This article discusses the possibility of using biometric information technology to authenticate users in information systems. Analyzed biometrics and identification system user. Recommendations on the use of various systems depending on the specific tasks.

Keywords: *biometrics authentication; biometrics; wavelet analysis.*

Введение. Биометрия – это наука, изучающая способы измерения различных параметров человека с целью установления сходства или различия между людьми и выделения одной конкретной личности из множества других. Слово «биометрия» переводится с греческого языка как «измерение жизни». Распознавание людей – это вид деятельности, который составляет основу нашего общества и культуры, так как для многих видов приложений необходимым условием является гарантия идентичности личности и ее авторизация. Биометрическая идентификация, или биометрия, основана на идентификации отличительных признаков человека. Таким образом, биометрия – это наука об идентификации или верификации личности по физиологическим или поведенческим отличительным характеристикам [1].

Биометрия как научное направление имеет специализированные направления теоретического и прикладного характера. В прикладном смысле биометрия рассматривается как метод идентификации человека, основанный на его физиологической или поведенческой характеристике. Физиологические биометрические параметры, такие, как отпечатки пальцев или геометрия руки, являются физическими характеристиками, которые обычно измеряются в определенный момент времени. Поведенческие биометрические параметры, например подпись или голос, представляют собой последовательность действий и длятся в течение определенного периода времени.

а) б)

Рис. 1.1. Отличительные индивидуальные характеристики: а) физиологические (отпечаток пальца); б) поведенческие (подпись)

Цель проводимого исследования. Надежная авторизация и аутентификация становятся необходимыми атрибутами овседневной жизни. Сегодня этот вопрос актуален даже при совершении самых простых действий, будь то регистрация на рейс, перевод денежных средств или просто проход в любое учебное учреждение. Возможность доступа часто принадлежит одному или нескольким людям. Установление личности не становится самой большой задачей, даже при необходимости высокой точности. Помимо этого, необходимо минимизировать вероятность отрицания пользователем проведенной им операции. Так же немало важной проблемой, о которой часто забывают разработчики, является пользовательский интерфейс и экстрактор биометрических данных. Они должны быть разработаны таким образом, чтобы испытывать минимум дискомфорта при прохождении процедуры аутентификации.

Таким образом, цель освещаемого в рамках данной статьи исследования можно определить следующим образом: разработка современной биометрической идентификационной системы, минимизированной по величине затрат временных ресурсов для процесса аутентификации личности, содержащей удобный пользовательский интерфейс и экстрактор биометрических данных.

Задачи. На данный момент перед биометрией стоит большое количество задач. В рамках проводимого исследования приводится рассмотрение следующие:

1. Уменьшение затрат временных ресурсов для процесса аутентификации личности.
2. Увеличение вероятности подлинной авторизации.
3. Поиск вариантов обезопасить владельцев биометрических параметров.

Область исследования. На данный момент существует три способа аутентификации:

– По собственности – физические предметы, такие как ключи, паспорт, смарт-карта и т.п.

– По знанию – информация, которой владеют лишь определенные личности. Знание обычно представляет собой какой-то пароль или парольная фраза. Но нужно заметить, что информация не должна быть обязательно секретной, например любимое блюдо или кличка питомца.

– По биометрическим параметрам – как уже говорилось это поведенческие или физиологические характеристики персоны.

Эти способы можно комбинировать, особенно. Вариант «пароль» + «идентификационный номер» объединяет в себе общеизвестные знания с секретной информацией. Например, банковская карта как собственность требует особых знаний для проведения операций, паспорт - это собственность с изображением лица и подписью, которые относится к биометрическим параметрам.

Аутентификацию в биометрии делят на два типа:

1. Верификация, основанная на биометрическом параметре и на уникальном идентификаторе, который выделяет конкретного человека (например, идентификационный номер), т.е. этот метод основан на комбинации аутентификационных приемов.
2. Идентификация, в свою очередь, основана только на биометрических измерениях. При этом измеренные параметры сравниваются со всеми записями из базы зарегистрированных пользователей, а не с одной из них, выбранной на основании какого-то идентификатора.

Вокруг биометрических исследований всегда было много споров и критики. Из-за большого внимания СМИ, биометрии приписывают чуть ли не магические свойства. Чтобы внести небольшую ясность для начала разберемся с ключевым понятием в этой области, таким как биометрические параметры. Под биометрическим параметром можно понимать любую особенность или признак, которой присущи следующие биометрические характеристики:

1. Всеобщность: каждый человек имеет биометрические характеристики.
2. Уникальность: для биометрии нет двух людей, обладающих одинаковыми биометрическими характеристиками.
3. Постоянство: биометрические характеристики должны быть стабильны во времени.
4. Измеряемость: биометрические характеристики должны быть измеряемы каким-либо физическим считывающим устройством.
5. Приемлемость: совокупность пользователей и общество в целом не должны (сильно) возражать против измерения/сбора биометрических параметров.[4]

Все эти свойства в совокупности определяют эффективность работы биометрических аутентификационных систем. Рассмотрим основные биометрические параметры, которые на сегодняшний день наиболее часто используются в автоматизированных аутентификационных системах. Это связанно с тем, что данные параметры считаются наиболее совершенными и удобными для точного измерения. Их в свою очередь для наглядности разделим на физиологические и поведенчиские:

Таблица 1

Наиболее часто используемые биометрические параметры

Физиологические	Поведенческие
Радужная оболочка глаза	Голос
Сетчатка глаза	Подпись
Геометрия руки	
Геометрия лица	
Отпечатки пальцев	

Так же существуют ещё некоторые другие биометрические параметры, которые используются реже, по причине их малой изученности. Среди них можно выделить следующие:

1. ДНК;
2. Форма ушей;
3. Запах;
4. Кожное отражение;
5. Термограмма;
6. Походка;
7. Клавиатурный почерк.

Чтобы максимально наглядно выразить ценность биометрического параметра, воспользуемся схемами Зефира. В них для сравнения разных биометрических параметров используются четыре свойства. Выбирая общие критерии для отбора, можно исключить биометрические параметры, не подходящие под них, основываясь на пороговых величинах области А.

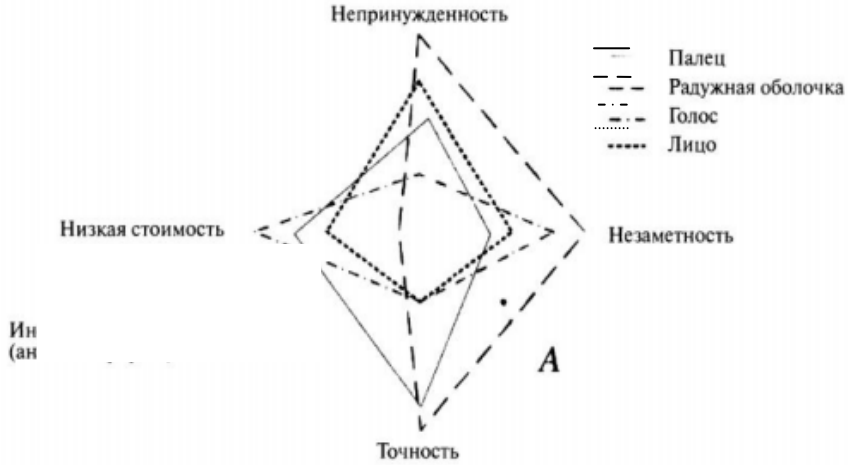


Рис. 1.2. Пример схемы Зефира

Рисунок 1.2. показывает сравнение таких биометрических параметров как палец, радужная оболочка, голос и лицо. Судя по графику, чем больше область определенного параметра, тем он лучше. Эта схема позволяет провести анализ по следующим свойствам:

1. Непринужденность – показатель легкости получения биометрического образца.
2. Незаметность – неудобство, связанное с использованием биометрического параметра.
3. Точность – точность биометрического параметра.
4. Низкая стоимость – стоимость оборудования для работы с данным параметром.

С помощью схем Зефира можем упорядочить параметры по убыванию величины определенного критерия:

Таблица 1.2

Биометрические параметры с точки зрения критериев отбора

Непринужденность	радужная оболочка > лицо > палец > голос
Незаметность	радужная оболочка > голос > лицо > палец
Точность	радужная оболочка > палец > лицо > голос
Низкая стоимость	голос > палец > лицо > радужная оболочка

Из всего этого следует, что каждый из биометрических параметров имеет как положительные так и отрицательные стороны. Использование того или иного параметра определяется спецификой той среды автоматизации, для которой он будет использован. В некоторых областях аутентификации бывает невозможно обойтись одним параметром, потому они так же могут использоваться в совокупности. Основное правило, регламентирующее использование тех или иных способов аутентификации, требует того, чтобы стоимость затрат на организацию доступа не превышала ценности хранимых ресурсов.

Математическое обеспечение. Для обработки биометрических параметров на данный момент самым актуальным решением является вейвлет-анализ. Это связанно с особенностями получения биометрических параметров. Физиологические биометрические параметры, такие, как отпечатки пальцев или геометрия руки, являются физическими характеристиками, которые обычно измеряются в определенный момент времени. А поведенческие биометрические параметры в свою очередь, например подпись или голос, представляют собой последовательность действий и длятся в течение определенного периода времени. Поведенческие биометрические параметры изменяются в течение

определенного периода времени, зависят от состояния человека и даже могут быть намерено изменены.

Таким образом, можно сказать, что физиологические биометрические параметры достаточно разнообразны и одного их образца обычно бывает достаточно для сравнения. Что касается поведенческих биометрических параметров, то отдельный образец может и не давать достаточных для идентификации личности сведений, но само временное изменение сигнала (под влиянием поведения) содержит необходимую информацию.

Вейвлеты были введены сравнительно недавно, в конце 1980-х. Вейвлет-анализ может быть охарактеризован как альтернатива классическому взвешенному анализу Фурье. Основными компонентами взвешенного анализа Фурье являются синусы и косинусы (волны), умноженные на скользящее окно. Они обычно называются частотновременными атомами. В вейвлет-анализе вместо умножения на синусы и косинусы этот вейвлет произвольно сдвигается и растягивается по временной оси. Таким образом, генерирующий вейвлет образует другие вейвлеты, которые являются строительными блоками вейвлет-анализа. Эти растяжения соответствуют различным степеням увеличения, а вейвлеты выполняют роль масштабно-временных атомов вейвлет-анализа.

Среди специалистов по численному анализу и обработке изображений принято считать, что величина, обратная масштабу, является частотой: малые масштабы соответствуют низким частотам, а большие масштабы соответствуют высоким частотам. Кроме того, значительно различающиеся масштабы должны давать независимую информацию о сигнале.

Вейвлеты неявно присутствовали в математике, физике, обработке сигналов и численном анализе задолго до того, как они получили статус отдельного научного направления [5]. Ещё одна важная область применения вейвлетов – сжатие изображений. На использовании техники вейвлетов базируется современная версия международного стандарта сжатия неподвижного изображения JPEG 2000 [6].

Из всего вышесказанного можно сделать вывод, теория вейвлетов является мощной альтернативой анализу Фурье и даёт более гибкую технику обработки сигналов. Одно из основных преимуществ вейвлет-анализа заключается в том, что он позволяет заметить хорошо локализованные изменения сигнала, тогда как анализ Фурье этого не даёт – в коэффициенте Фурье отражается поведение сигнала за всё время его существования. Но в то же время в вейвлетах широко используется техника рядов Фурье и преобразования Фурье [7].

Заключение. Биометрия как наука имеет множество граней, с которых можно её рассматривать. Однозначно дать ответ на то, какой параметр лучше подходит для аутентификации, никак нельзя, в виду их индивидуальных особенностей. Решением данной задачи может стать комбинация параметров, которая сведет к минимуму вероятность ложной аутентификации.

Не стоит так же забывать об удобстве пользователей. Излишний дискомфорт может отрицательно настроить и без того скептически настроенных пользователей. В связи с этой проблемой начинают изучать такие биометрические параметры, как походка человека или геометрия лица. Эти способы помогут установить личность человека без его непосредственного участия.

Правильно выбранная и оптимизированная математическая модель обработки биометрических параметров сможет увеличить скорость работы аутентификационных интерфейсов, а также уменьшить риск ложного доступа к системе.

СПИСОК ЛИТЕРАТУРЫ

1. Руководство по биометрии: монография / Болл Р.М. [и др.] - М.: Изд-во «Техносфера», 2007.- 368 с.
2. Двоеносова Г. А. Биометрия как наука, метод и способ документирования / Двоеносова Г. А. Двоеносова М. В. // Управление персоналом - 2009 - № 11 - С.82-86.
3. Миллер Б. Существенные признаки идентичности //Американский научно-технический журнал – 1994.
4. Кларк Р. Идентификация человек в информационных системах: проблемы управления и общественно-политическим вопросам // Информационные технологии и люди – 1994 - №3 – с. 6-37
5. Блаттер К. Вейвлет анализ. Основы теории : монография - М.: Изд-во «Техносфера», 2006.- 272 с.
6. Штарк Г.Г. Применение вейвлетов для цифровой обработки сигналов - М.: Изд-во «Техносфера», 2007.- 192 с.
7. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB. – М.:ДМК Пресс, 2008 – 448 с

УДК 681.2

АНАЛИЗ СИСТЕМНЫХ АСПЕКТОВ УПРАВЛЕНИЯ РАЗВИТИЕМ КРИТИЧЕСКИХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Волков Виктор Иванович, Тычинин Игорь Юрьевич, Алексеев Анатолий Владимирович,
Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова,
Санкт-Петербург, Россия, Ушаковская наб., д. 17/1, ВУНЦ ВМФ «ВМА»
e-mail: iapbgks@bk.ru

Аннотация: Рассмотрены системные аспекты развития критических объектов морской техники и морской инфраструктуры. Показано, что в современных условиях их развития первостепенное внимание при наращивании их возможностей и качества следует уделять именно системным

требованиям, характеристикам и их оптимизации. Это обусловлено лавинообразным возрастанием структурной и алгоритмической сложности объектов, ужесточением требований по качеству процессов их концептуального, исследовательского, эскизного, технического и конструкторского проектирования, технологической подготовки и организации производства, проведения испытаний на всех стадиях создания новых образцов техники и их модернизации. А также качественно новыми требованиями к подготовке обслуживающего персонала и выполнению ими функциональных обязанностей в строгом соответствии с установленными регламентами. Приведены конкретные примеры реализации данных системных требований на базе технологических решений и программных комплексов, зарегистрированных в ФСИС РФ.

Ключевые слова: *информационные технологии, конкуренция, критические объекты, управление развитием, системные характеристики, интеллектуализация управления.*

ANALYSIS OF THE SYSTEMIC ASPECTS OF MANAGEMENT DEVELOPMENT CRITICAL INTEREST IN MARINE ENGINEERING AND MARINE INFRASTRUCTURE

Viktor Volkov, Igor Tichinin, Anatoly Alekseev,
Military training and scientific center of the Russian Navy «Naval Academy. N.G. Kuznetsov»,
St. Petersburg, Russia, is the name of embankment, D. 17/1

Abstract: We consider a system aspects of the development of critical objects in marine engineering and marine infrastructure. It is shown that in modern conditions of their development priority when building their capabilities and quality should be given to the system requirements, performance and optimization. This is due to the exponential increase in structural and algorithmic complexity, the stricter requirements for the quality of their conceptual processes, research, conceptual, technical, and engineering design, technological preparation and organization of production, testing at all stages of the design process and their modernization. As well as qualitatively new requirements for training operating personnel and the performance of their functional duties in strict accordance with the established regulations. Specific examples of the implementation of the data system requirements on the basis of technological solutions and software systems, registered in the FSIS of the Russian Federation.

Keywords: *nformation technology, competition, critical facilities, development management, system characteristics, intellectualization management.*

Введение. Современные объекты морской техники и морской инфраструктуры (ОМТИ) типа атомные суда, нефтеналивные суда, в том числе ледового класса танкеры, газовозы, химовозы и т.п., морские ледостойкие стационарные платформы типа «Приразломная» и другие, характеризуются целым рядом качественно новых свойств, определяемых спецификой внедряемых новых технологий.

Среди них определяющая роль сегодня, безусловно, принадлежит информационным технологиям (ИТ). Качественно новые возможности информационно-коммуникационных систем, систем обработки и визуализации информации открыли принципиально новые горизонты по масштабному расширению спектра функциональных возможностей и границ автоматизации, по миниатюризации средств и систем ОМТИ, по уровню и качеству используемых сервисов [1].

Вместе с тем, это привело к лавинообразному возрастанию структурной и алгоритмической сложности автоматизированных средств и систем ОМТИ, в том числе в защищенном исполнении (АСзи). Как следствие, это привело к ужесточению требований по качеству процессов концептуального, исследовательского, эскизного, технического и конструкторского проектирования, технологической подготовки и организации производства, изготовлению АСзи, проведению испытаний на всех стадиях создания новых образцов ОМТИ и их модернизации [2]. Тем не менее, специфика новых социально-экономических отношений в стране привела к определенному технологическому «упрощению» производственно-технологических отношений, резкому снижению практических требований к качеству и требованиям регламентирующих документов, к качеству процессов, продукции и услуг в целом [3].

Наконец, объективное требование к повышению уровня и качества подготовки персонала, обслуживающего эти сложные эрготехнические комплексы и системы (ЭТС), выполнению им функциональных обязанностей в строгом соответствии с установленными техническими регламентами (число которых, кстати сказать, в последнее время стало также резко возрастать) вошло в противоречие с обратной тенденцией. Практического снижения престижности многих технических специальностей, уровня знаний при подготовке и переподготовке специалистов, уровня научно-технического обоснования и развития соответствующих сегментов знаний. Одной из причин тому следует считать резкое возрастание объема использования импортного оборудования, что, естественно, привело к существенному снижению востребованности профессий разработчиков и проектировщиков, испытателей новых средств и широких слоев научно-технического персонала [4].

В сочетании с названными факторами анализ многих других аспектов управления развитием современных ЭТС позволяет утверждать, что большинство из ОМТИ следует рассматривать сегодня,

прежде всего, как критически важные объекты повышенного риска. При этом, реализуемые в них современные ИТ относятся к числу ключевых, т.е. нарушение (или прекращение) функционирования которых приводит к потере на длительный период времени управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) прогрессивного развития экономики отрасли, субъекта или административно-территориальной единицы, или существенному ухудшению безопасности жизнедеятельности персонала ОМТИ, угроз техногенного, природного характера и различных вариантов террористических проявлений [5].

Высокая критичность ИТ ОМТИ к внешним (условия среды использования) и внутренним (условия среды обеспечения функционирования, включая обусловленные негативным влиянием субъективных свойств операторов) факторам сегодня, как правило, «нейтрализуется» по пути повышения аппаратно-программной надежности используемых элементов и ОМТИ в целом и, главное, по традиционному пути резервирования контуров управления, повышения степени автоматизации решаемых в них задач. Но, кроме того, по пути повышения надежности, качества решения функциональных задач самым слабым звеном в автоматизированных контурах управления – лицами, принимающими управленческие решения (ЛПР), их обосновывающими (ЛОР) и исполняющими (ЛИР) с присущими им, как позитивными, так и рядом негативных свойств и факторов. Т.е. операторов (в широком смысле этого термина) и, прежде всего, за счет совершенствования систем информационной, аналитической и интеллектуальной поддержки принятия решений (СИП) операторами в ключевых контурах автоматизированного управлениях [6].

Особо критичными в этих условиях, как показывает многочисленная практика, является, с одной стороны, системное обоснование, а, с другой стороны, реализация и выполнение при эксплуатации системных требований к ОМТИ. К их числу, прежде всего, относятся:

1. Требования по составу достигаемых АСзи ОМТИ целей и адекватности вытекающих из них соответствующих функциональных задач, их непротиворечивости и достаточности для обеспечения требуемой валидности (обязательности достижения комплекса декларируемых целей).

2. Требования по структуре (архитектуре) АСзи ОМТИ, её оптимизации и безизбыточности, обоснованности и качества выбранных или разрабатываемых элементов с комплексом соответствующих свойств и характеристик.

3. Требования по взаимосвязи (согласованности, гармоничности) элементов в составе АСзи ОМТИ, качеству (проектному) и эффективности (реализуемому при эксплуатации проектному качеству) решения функциональных задач (требования по предназначению).

4. Требования по верификации декларируемых и практических (обеспеченных) системных требований АСзи ОМТИ на всех этапах их жизненного цикла, включая, как этап создания опытных образцов и всесторонних их испытаний, так и во всех фазах их эксплуатации.

5. Требования по составу и уровню обоснованности формируемых новых требований к качеству АСзи ОМТИ в процессе и интересах обеспечения их эволюционного, либо революционного развития (резкого по наращиванию качества, архитектуре, составу, функциям, взаимосвязи и т.п.), а главное – обеспечения конкурентной способности (КС) и конкурентных преимуществ (КП).

В названный комплекс системных требований к АСзи ОМТИ, как правило, традиционно входят также конкретные требования по устойчивости их функционирования (надежности, робастности и др.), требования по ресурсной затратности (организационной, временной, финансовой, материально-технической, трудовой и др.).

Кроме того, также требования по безопасности эксплуатации (обслуживания, службы персонала, экологической и др.), управлению аварийными ситуациями и авариями, а также борьбой за живучесть ОМТИ (прежде всего, корабля, судна), как их способностью противостоять последствиям аварийных повреждений, восстанавливая и поддерживая при этом в достаточной мере свои функциональные качества. Для судов, в первую очередь, мореходные качества.

Весь этот комплекс системных требований должен быть обеспечен соответствующими методологическими и организационно-распорядительными решениями, комплексом документации, а также комплексом аппаратно-программных средств оценки, анализа и мониторинга достигаемого уровня системного качества и эффективности АСзи ОМТИ. АСзи, как сложной эрготехнической (человеко-машинной) и организационно-технической совокупности взаимосвязанных элементов системы (подсистем, комплексов, устройств и т.п.), обеспечивающих во взаимосвязи решение общесистемных задач и достижение общесистемных целей.

В этих условиях, не взирая на известную структурную и функциональную сложность ОМТИ, а также, как следствие, методологическую сложность моделирования функционирования и оценки качества, имеет место негативная практика и тенденция количественной оценки качества только в части отдельных элементов без количественной оценки качества системы элементов в целом.

Такой подход и практика, обусловленные, как правило, «осторожностью» Разработчика и его стремлением упрощать процедуру сдачи Заказчику готовой продукции, являются заведомо ошибочными в системном аспекте, т.к. исключают возможность практической проверки, оценки и контроля валидности результатов. Под ней понимается при условии выполнения опытным образцом (изделием) поставленных в техническом задании (ТЗ) на научно-исследовательскую (НИР) или

опытно-конструкторскую (ОКР) работу функциональных задач проверка степени достижения поставленных в ТЗ целей, т.е. проверка одного из главных системных требований.

С другой стороны, замена конкретных квалиметрических оценок (оценок по измерению уровня качества), как это часто встречается практически, расчетной, либо экспертной оценкой возможности решения системных задач и достижения системных целей ОМТИ на уровне комиссий по приемке НИОКР (даже при наличие фрагментарных данных модельных экспериментов) не может быть адекватным эквивалентом. Это порождает, как правило, новые системные риски: фактической незавершенности выполняемых НИОКР; фактической невозможности адекватной оценки достигнутых результатов и эффективности ресурсных затрат; фактического отсутствия научно-методической «прозрачности» управления направлениями развития критических ОМТИ.

Другим важным системным аспектом управления современными критическими ОМТИ следует считать, как известно, существенно более высокий и критический уровень риска, ресурсных затрат и потенциального ущерба при принятии ошибочных системных управленческих решений, в том числе при определении направлений развития соответствующих технологий и решений [7].

В этих условиях в дополнение к уже названному системному требованию обязательной количественной оценки качества ОМТИ в фактических условиях принятия решений следует считать целесообразным проведение квалиметрической сертификации перспективных технологических решений, формирование на их основе соответствующих баз данных и знаний с оценкой их конкурентной способности [8-9]. В этих условиях разработка планов и программ перспективного развития передовых технологий и ОМТИ в целом в системном аспекте управления развитием АСзи представляется существенно более простым, естественным и перспективным процессом, включая форсированное решение проблем влияния субъективных («человеческих») факторов [10].

Наконец, пожалуй, самым значимым системным аспектом современного управления критическими ОМТИ является минимизация их информационной, структурной, функциональной избыточности за счет решения задачи многокритериальной и полимодельной оптимизации с «полномасштабным» использованием всего «арсенала» современных научных достижений.

При этом, под информационной δИ (структурной δС, функциональной δФ) избыточностью понимается мера возможного сокращения объема информации ΔI (числа структурных элементов в составе системы ΔN, числа решаемых функциональных задач ΔF с соответствующими межэлементными связями ΔZ), при котором с заданной точностью ΔQДОП не ухудшается качество системы Q ≥ QТЗ , где QТЗ – значение качества системы, определяемое требованиями ТЗ.

В процессе решения задач системного анализа и последующего синтеза АСзи ОМТИ именно поиск такого сочетания характеристик, при котором обеспечивается максимизация показателя качества Q → Max и минимизация избыточности δ(δС, δФ, δИ, …) является, как можно показать, наиболее значимым критерием проектирования АСзи ОМТИ и, прежде всего, вариантного.

Это важное понятие и соответствующий критерий проектирования АСзи ОМТИ δ → Min будут только тогда иметь значение, если будет доступен аппарат моделирования главного показателя любой системы, а именно – критерия (меры соответствия предназначению) и показателя (численного выражения критерия) её качества Q. Однако, широко распространенных и общепризнанных методических решений этой научно-технической задачи применительно к конкретным практическим задачам сегодня крайне мало. В то время, как значимость вопроса стремительно возрастает.

Одним из перспективных направлений и методов решения задач данного класса наряду с эврестическими методами, методом паритета, линейно-экспоненциальными методами и подобными, следует считать уже достаточно изученные так называемые формальные методы решения многокритериальных задач на основе агрегирования векторных критериев [11].

В настоящее время известен целый ряд алгоритмов агрегирования частных показателей качества (ЧПК) в групповые (ГПК), модельные (МПК) и агрегированный (сводный) показатель качества (АПК, СПК). В систематизированном виде они приведены в таблице из [11] с тем отличием, что в нее добавлен становящийся весьма предпочтительным в последнее время так называемый метод гармонической оптимальности [12]. Он удачно сочетает в себе преимущества аддитивного алгоритма с мультипликативным. При этом, получаемые оценки по этому алгоритму занимают компромиссное промежуточное положение между оценками по образующим его методам.

Таблица 1

Основные методы агрегирования векторных критериев и оптимизации решений

Методы агрегирования векторных критериев	**Математическая модель алгоритмов агрегирования**	**Сравнительные свойства, рекомендации**
1. Метод равномерной оптимальности (МРО)	Аддитивный алгоритм свёртки ЧПК $\mathbf{W_k}$ с весовыми коэффициентами $\mathbf{q_k}$ вида: $\mathbf{W_A = \sum_k (q_k * W_k)}$	Определение весовых коэффициентов методом (МСП) или рондомизированных (МРСП) сводных показателей
2. Метод справедливого компромисса (МСК)	Мультипликативный алгоритм свёртки ЧПК $\mathbf{W_k}$ с весовыми коэффициентами $\mathbf{B_k}$ вида: $\mathbf{W_M = \Pi (W_k^{Bk})^k}$	Определение весовых коэффициентов МСП или МРСП

3. Метод гармонической оптимальности (МГО)	Гармонический алгоритм свёртки: $W_Г = (W_A * W_M)^{0,5}$	Одновременное сочетание преимуществ МРО и МСК
4. Метод гарантированного результата (МГР)	Алгоритм максимизации минимальной эффективности: $W_{ГР} = \underset{J}{Max} [\underset{k}{Min} (W_k)]$	Тактика «замораживания» (пессимистического) резервов развития
5. Метод максимальной эффективности (ММЭ)	Алгоритм максимизации максимальной эффективности: $W_{МЭ} = \underset{J}{Max} [\underset{k}{Max} (W_k)]$	Тактика «фиктивной» (оптимистической) эффективности
6. Метод фиксированных ограничений (МФО)	Алгоритм перевода **(k-1)** критериев в ограничения кроме **k = g**: $W_{ФО} = \underset{J}{Extr}\, W_g ,\quad W_k > W_{k_min}$	Проблема оценки допустимых ограничений W_{k_min}
7. Метод последовательных уступок (МПУ)	Алгоритм последовательных уступок Δ_k по **(k-1)** критериям кроме **k = g**: $W_{ПУ} = \underset{j}{Extr}\, W_g ,\quad W_k = W_k - \Delta_k$	Проблема оценки допустимых уступок Δ_k
8. Метод эвристических решений (МЭР)	Алгоритм формируется и оптимизируется ЛПР: $W_{ЭР} = Opt \{ ЛПР, Extr [W_{э,k}] \}$	Проблема синтеза ЛПР структуры алгоритма $W_{э,k}$
9. Метод идеальной точки (МИТ)	Алгоритм идеальной точки: $J_{opt} = \underset{j}{Arg\ Min}\ Dist (W_j , W_{max})$	Проблема синтеза идеальной точки W_{max} , точности оценок
10. Метод анализа и синтеза при информационном дефиците (АСПИД)	На основе алгоритма равномерной оптимальности с использованием метода имитационного моделирования для оценки весовых коэффициентов	Программная реализация метода АСПИД: «ASPID-W», «APIS»
11. Метод анализа иерархий (МАИ)	На основе алгоритма равномерной оптимальности с использованием 9-уровневой модели предпочтений для оценки весовых коэффициентов	Вариант программной реализации МАИ: «MPRIORITY»
12. Полимодельный метод (ПММ)	Одновременное использование нескольких методов, моделей предпочтений, вариантов условий и оценивания с агрегированием получаемых оценок	Взаимная верификация и актуализация моделей, условий и оценок ПУР
13. Метод квалиметриической ранговой оптимизации (КРОПУР)	Многовариантная многокритериальная полимодельная оценка, анализ и оптимизация обоснования выбора решения с ранжированием вариантов	Типизация моделей пре-дпочтений с ранжированием оценок и решений
14. Метод анализа, синтеза и вариантной оптимизации ПУР (АСОР)	Многовариантная КРОПУР с синтезом и оптимизацией решений на основе метода корневой чувствительности и их многомерной визуализацией	Типизация формализованного представления задачи синтеза ПУР

Поскольку каждый из предлагаемых методов базируется на соответствующих модельных ограничениях, а стало быть, приводящих к соответствующим методическим погрешностям, особый интерес и, особенно, для сложных ЭТС, представляет так называемый полимодельный метод. Он основан на одновременном использовании нескольких моделей и вариантов условий оценивания с соответствующим взвешиванием оценок и используемых моделей. Такой подход, как показывает практика, позволяет существенно снижать методические погрешности оценивания, соответствующие модельные ограничения. Более того, этот подход позволяет обоснованно применять и наращивать возможности исходных методов с учетом их позитивных и специфических (негативных) свойств.

Именно этот подход реализован в методе и одноименной автоматизированной системе поддержки принятия решений (АСППР) на базе программного комплекса «Программа квалиметрической ранговой оптимизации проектных и управляющих решений (КРОПУР)», зарегистрированной в Федеральной службе интеллектуальной собственности (ФСИС) за №2013612649, 11.03.2013.

В контексте названных проблемных аспектов управления развитием АСзи ОМТИ конкретные варианты реализации приведенных системных требований использованы в технологических решениях и программных комплексах [1,3,6,10,12], также зарегистрированных в ФСИС за номерами:

– 2013612363, 26.02.2013, «Программа имитации сигналов контроля состояния общесудовых систем по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля (ИП.1)»;

– 2013612929, 18.03.2013, «Программа квалиметрического анализа и оценки конкурентной способности технологических решений по информационной поддержке принятия решений судоводителем (QSWOT)»;

– 2014613608, 31.03.2014, «Программный модуль экспертного квалиметрического оценивания уровней технологических решений по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля, судна (МКО)»;

– 2014613622, 1.04.2014, «Автоматизированная система информационно-аналитической и интеллектуальной поддержки операторов при мониторинге, оценке обстановки, контроле и управление состоянием организационно-технических систем по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля, судна (АСИП МОКУ)»;

– 2014613624, 1.04.2014, «Адаптивное прогнозирование развития данных в каналах контроля технического состояния судовых систем по безопасности эксплуатации, локализации аварий и борьбе за живучесть корабля, судна (АПД)»;

– 2014613724, 28.08.2014, «Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО о3)».

Комплексная математическая модель поддержки принятия решений ЛОР, ЛПР, ЛИР, как одной из критических задач управления современными сложными ЭТС [10], [11], [12], приведена на рисунке 1.

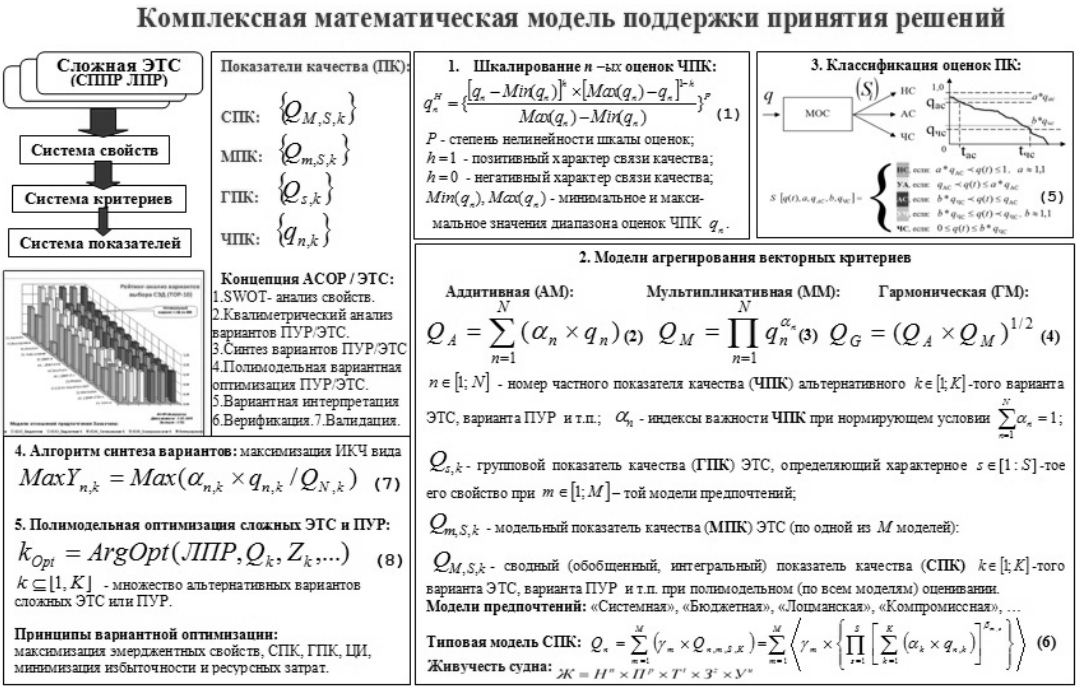


Рис. 1. Комплексная математическая модель поддержки принятия решений: системные аспекты

В данной модели учтены и реализованы многие из сформулированных выше системных требований и аспектов управления развитием АСзи ОМТИ, в том числе в форме АСППР «АСИП МОКУ», «ПК МДО СИП ЛА-ГО о3» и отдельных технологических решениях «ИП.1», «АПД» [1, 12].

При этом, к числу основных системных аспектов управления качеством поддержки принятия решений ЛОР, ЛПР, ЛИР, приобретающих концептуальный характер [1,3-12], следует отнести:

– агрегирование ЧПК в ГПК, МПК и СПК (АПК), их визуализация и мониторинг в реальном масштабе времени с оперативным и упреждающим управлением качеством функционирования АСзи;

– синтез вариантов АСзи ОМТИ на основе максимизации индексов корневой чувствительности (ИКЧ), определяемых соотношением системных показателей типа СПК и ЧПК;

– оптимизация сложных ЭТС и принимаемых проектных (при создании) и управленческих (при эксплуатации) решений на основе максимизации СПК (АПК) АСзи ОМТИ и их прогнозирования;

– малоизбыточная визуализация данных в составе ключевых ГПК, МПК и СПК (АПК) для обеспечения сопряжения всего комплекса эрготехнических характеристик ОМТИ, включая АСзи;

– максимизация качества информационно-аналитической и интеллектуальной поддержки принятия решений на основе автоматической (оперативной) оценки и мониторинга в реальном масштабе времени ключевых системных показателей качества по каждому из элементов и АСзи ОМТИ в целом с учетом возможности их прогнозирования.

В результате выполненного анализа системных аспектов управления развитием критических объектов морской техники и морской инфраструктуры могут быть сделаны следующие выводы:

1. В современных условиях развития ОМТИ и их АСзи первостепенное внимание при наращивании их возможностей и качества, для обеспечения конкурентной способности и конкурентных преимуществ, следует, прежде всего, уделять именно их системным требованиям и характеристикам, в том числе их верификации и оценке валидности при испытаниях.

2. Их оптимизацию при проектировании АСзи в составе ОМТИ, а также в процессе эксплуатации при мониторинге в реальном масштабе времени в обеспечение эффективной эксплуатации следует рассматривать в качестве ключевого условия эффективного управления развитием средств автоматизации и ОМТИ в целом, обеспечения их конкурентных преимуществ.

3. Современный уровень развития отечественных информационных технологий управления развитием систем автоматизации ОМТИ, как сложных и критических эрготехнических систем, при условии методологически и научно-технически обеспеченном принятии проектных и управленческих решений позволяет уже сегодня ставить и успешно решать задачу создания конкурентно способных отечественных средств и систем ОМТИ, а также их эффективного применения.

СПИСОК ЛИТЕРАТУРЫ

1. Волков В.И., Тычинин И.Ю., Алексеев А.В. Системные аспекты управления развитием современных критических объектов морской техники и морской инфраструктуры – 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. С. 447-448.
2. Морская радиоэлектроника: Справочник / И.В. Соловьев, Г.Н. Корольков, А.А. Бараненко, М.Н. Баранов, А.В. Алексеев, Л.С. Васильев и др.; Под ред. В.А. Кравченко. СПб.: Политехника, 2003. – 246 с.
3. Алексеев А.В. Технология и программный комплекс квалиметрической ранговой оценки качества сложных информационно-аналитических систем / Материалы IX Всероссийской научно-практической конференции МОРИНТЕХ-ПРАКТИК «Информационные технологии в судостроении–2008». – СПб., ОАО «Северные верфи»,19.06.2008, с.110–118.
4. Алексеев А.В. Управление технической системой безопасности в промышленности / Системы безопасности. Журнал для руководителей и специалистов в области безопасности, 2004, №6 (60), с. 68 – 73.
5. Алексеев А.В., Орлов К.М. Информационно-аналитическое обеспечение современных специальных информационно-управляющих комплексов: состояние, проблемы и перспектив развития. Статья, сборник «Состояние, проблемы и перспективы разработки корабельных информационно-управляющих комплексов. / Сборник докладов научно-технической конференции. – М.: ОАО «Концерн «Моринформсистема-Агат», Москва, 2010, с.69-75.
6. Алексеев А.В. Методология синтеза системотехнических решений автоматизации процессов борьбы за живучесть судов повышенного риска /Актуальные проблемы морской энергетики: материалы третьей Всероссийской межотраслевой научно-технической конференции. – СПб.: Изд-во СПбГМТУ, 2014, с. 181 с.
7. Алексеев А.В. Оптимизация проектных и управленческих решений при комплексном обеспечении безопасности большого города // Безопасность большого города / Сб. ст.под ред. Э.И.Слепяна. – Санкт-Петербург: Издательство Сергея Ходова, 2007, с. 400-418.
8. Смольников А.В, Алексеев А.В., Антипов В.В., Бобрович В.Ю. Ранговая сертификация современных эрготехнических систем, как реальный способ повышения конкурентоспособности объектов морской техники и морской инфраструктуры – Морской Вестник, 2013, №1 (10), с. 55 - 59.
9. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор». Спб., 7-9.10.2014 – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С. 29-34.
10. Алексеев А.В. Технология квалиметрической ранговой оптимизации проектных и управленческих решений» / Труды Международной Научной Школы «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР-2007)» – Спб., ГОУ ВПО «СПбГУАП» 2007. – с. 285 – 290.
11. Основы проектирования систем защиты информации – СПб.: СПбГМТУ, 2008 г. – 71 с. (с. 40).
12. Алексеев А.В. Перспективы развития технологий управления электроэнергетическими системами танкерного флота /Актуальные проблемы морской энергетики: Материалы четвертой Всероссийской межотраслевой научно-технической конференции. Посвящается 125-летию профессора, д.т.н., заслуженного деятеля науки и техники В.А. Ваншейдта. – СПб.: Изд-во СПбГМТУ, 2015. – 205 с. (С. 92-95).

УДК 681.2

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ОПЕРАТИВНОГО ДИАГНОСТИРОВАНИЯ СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ

Грищенко Дмитрий Вячеславович,
Санкт-Петербургский государственный морской технический университет,
Санкт-Петербург, Россия, ул. Лоцманская, дом. 3,
e-mail: tstf@mail.ru

Аннотация: В статье рассмотрены результаты разработки стационарной системы непрерывного контроля технического состояния и оперативной диагностики судового роторного оборудования, описана ее структура и общие принципы функционирования ее модулей.

Ключевые слова: *система; сигнал вибрации; диагностика; анализ; тренд; спектр.*

INFORMATION-MEASURING SYSTEM OF RAPID DIAGNOSTICS ROTARY SHIPBOARD MACHINE

Dmitriy Grishchenko,
St. Petersburg State Marine Technical University,
Russia, Lotsmanskaya Street 3, St. Petersburg,
e-mail: tstf@mail.ru

Abstract: The results of online system for continuous machine condition monitoring and diagnostics of rotating marine equipment are discussed; the architecture of such systems and general principles of its modules functioning is described.

Keywords: *system; vibration signal; diagnostics; analysis; trend; spectrum.*

Введение. Информационно – измерительные диагностические технологии и системы широко и эффективно используются на многих производствах. Подобные системы, предназначенные для работы с роторным оборудованием, как правило, основаны на вибрационном методе, который имеет ряд преимуществ по сравнению с другими методами неразрушающего контроля: высокая информативность, мгновенная реакция на изменение состояния, возможность обнаружения дефектов на ранней стадии развития, сравнительная простота измерения, возможность локализации дефекта.

Существует два основных направления применения таких технологий в производстве. В первом случае системы используются для эффективного управления предприятием, при этом получаемая информация о состоянии оборудования используется для оптимизации обслуживания и ремонта, а также обеспечения безотказности сравнительно простых, как правило, однорежимных агрегатов, которые непосредственно не управляются оператором. Для этих целей измерения обычно проводятся с малой периодичностью (для исправных агрегатов – раз в 2–3 месяца), а в качестве инструментов используются переносные средства глубокой диагностики и экспертные программы. Во втором случае получаемая диагностическая информация используется для эффективного управления непосредственно оборудованием, в том числе для обеспечения его защиты от внезапных отказов, которые чаще всего возникают из-за ошибок управления или нарушений в технологическом процессе. Для данных целей используются стационарные системы с высокой периодичностью получения данных измерений. Такие системы могут быть автоматическими – т.е. непосредственно связанными с системой управления агрегатом, или диспетчерскими – информационные системы для предоставления информации оператору.

Рассматриваемая разработанная система является диспетчерской информационной системой нового поколения, которая выполняет следующие функции, как в условиях промышленного производства, так и при установке на борту судна:

– непрерывный контроль технического состояния оборудования в установившихся и переходных режимах работы с идентификацией изменений состояния вследствие ошибок управления,

– оперативная диагностика при обнаружении изменения состояния с идентификацией развитых дефектов, прогнозом остаточного ресурса и выдачей рекомендаций обслуживающему персоналу,

– сбор первичных сигналов для диагностической службы предприятия (береговой службы) в целях проведения глубокой диагностики и планирования обслуживания.

Структура системы представлена на рисунке 1. В состав системы входят измерительные преобразователи вибрации и тока, а также датчики оборотов. Сигнал вибрации, измеренный на опорах вращения и корпусах роторного оборудования, является основным источником информации для принятия решений, однако анализ сигнала тока также позволяет получить большой объем диагностической информации, связанной с состоянием не только непосредственно электрической машины, силовой ток которой измеряется, но и приводного агрегата.

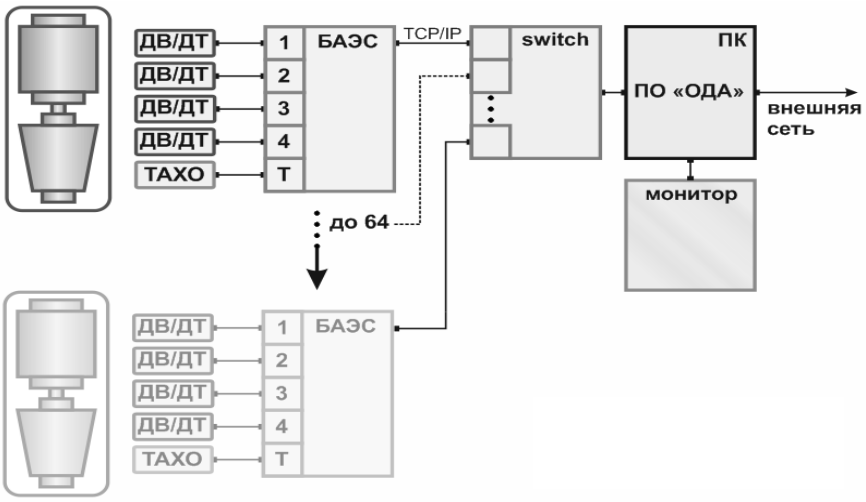


Рис. 1. Структура системы оперативного диагностирования.

Сигналы с измерительных преобразователей поступают на вход измерительных модулей системы – БАЭС (блок анализа электрических сигналов), в которых происходит их оцифровка и анализ, далее результаты анализа выдаются в измерительную сеть в виде пакетов с данными, которые принимает компьютер с программой ОДА (оперативная диагностика агрегатов).

Для каждого виброизмерительного канала производятся вычисления следующих вибропараметров: уровень виброскорости в полосе от 10 до 1000 Гц, третьоктавный спектр вибрации в диапазоне частот от 5 Гц до 10 кГц, узкополосный спектр до 10 кГц, СКЗ и пиковое значение высокочастотной (выше 8 кГц) импульсной вибрации. В каналах измерения тока измеряются узкополосные спектры тока до частоты 10 кГц. Используемые виды анализа вибрационных и токовых сигналов оптимизированы для решения задач оперативного обнаружения изменения состояния и идентификации развитых дефектов роторного оборудования с высокой достоверностью.

При этом с постоянной периодичностью в 1,6 сек. в информационную сеть выдаются результаты измерений без узкополосных спектров (малые пакеты данных), а совокупность всех видов анализа (большие пакеты) выдается по запросу, который формируется либо с некоторой периодичностью, либо по событию при превышении порогов данных малых пакетов.

Пакеты с данными через информационную сеть поступают в программу ОДА, структура которой представлена на рис. 2. Каждый параметр попадает в предварительный накопитель на 8 измерений (12,6 секунды), в котором анализируются быстроизменяющиеся процессы. Далее усредненные определенным образом данные попадают в следующие три последовательных накопителя на 64 измерения разной длительности (накопители быстрого и медленного мониторинга и блока диагностики). Накопители выполнены в виде принципа «первый пришел – последний вышел». Длина по времени каждого накопителя соответствует типовой длительности различных переходных режимов работы – мгновенного и плавного пуска, выхода на режим, установления теплового равновесия. Это позволяет анализировать тренды разной длительности и разделять изменения состояния, связанные с различной скоростью деградации, и естественные флуктуации параметров, связанные с переходными режимами работы контролируемого агрегата. По результатам анализа трендов в конкретном накопителе определяется базовый уровень для адаптации порога в накопителе меньшей по времени длительности. Такой подход позволяет отстроиться от медленных изменений внешних условий и изменений режима работы оборудования, сохраняя высокую чувствительность обнаружения быстрых изменений состояния, в том числе из-за ошибок управления агрегатами. В свою очередь, монотонные измерения состояния агрегата в результате естественного старения уверенно обнаруживаются по анализу усредненных данных в последнем накопителе (архив базы данных), в котором хранятся данные за все время работы системы.

В накопителе на 8 измерений анализируется тренд, определяемый по всем данным накопителя, при анализе трендов на 64 измерения применяется другой подход, обусловленный возможностью возникновением в пределах накопителя интервалов данных, связанных с различными режимами или условиями работы. Для обнаружения таких интервалов производится построение тренда с обеих сторон накопителя пошагово, начиная с первых (последних) 10 измерений, при этом каждый раз проверяется условие на обрыв тренда, если условие не выполняется, то интервал для построения тренда увеличивается на 1 измерение и условие на обрыв проверяется снова.

Такими условиями могут быть суммарное отклонение от прогноза следующими за трендом 3-мя значениями – рисунок 3, сильный скачек следующего значения и увеличение разброса по следующим 5-ти значениям. Несовпадение трендов, построенных с начала и конца накопителя означает наличие точек перегиба и, возможно, нестабильности (сильный разброс данных).

Для каждой возможной ситуации (наличие участков с различной направленностью трендов, нестабильности) предусмотрен способ определения базового значения по накопителю, которое является опорным для построения порогов в предшествующем по длительности накопителе. Также такой подход позволяет оценить последствия работы в нежелательных режимах, которое определяется как разница между горизонтальными трендами до и после нестабильного режима**.** В каждом накопителе производится сравнение данных с порогами, на основании данного сравнения, а также характеристик тренда определяется степень опасности по данному параметру. Степень опасности для конкретной точки контроля – интегральная оценка опасности всех измеренных параметров этой точки.

Режим идентификации дефектов запускается периодически и по событию, при превышении одним из контролируемых параметров вибрации пороговых значений или появлении скачка. Диагностика осуществляется по параметрам, превысившим один или несколько соответствующих пороговых значений и по трендам развития этих параметров (прогнозируемому времени достижения ближайшего порога). Задача сводится к определению наиболее вероятных дефектов из множества возможных. Это множество состояний предварительно составляется и закладывается в диагностический модуль в виде матриц с коэффициентами влияния. В качестве вибродиагностических параметров используются как уровни суммарной вибрации в разных полосах, так и параметры выделенных из спектров вибрации периодических и случайных компонент.

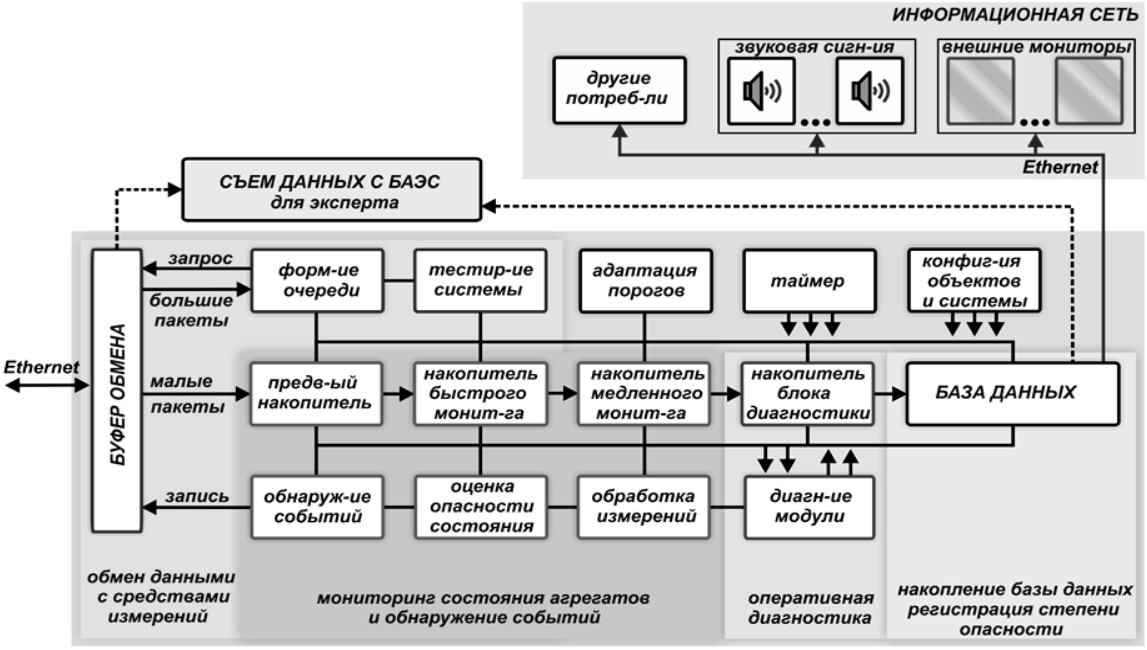


Рис. 2. Структура диагностической программы ОДА

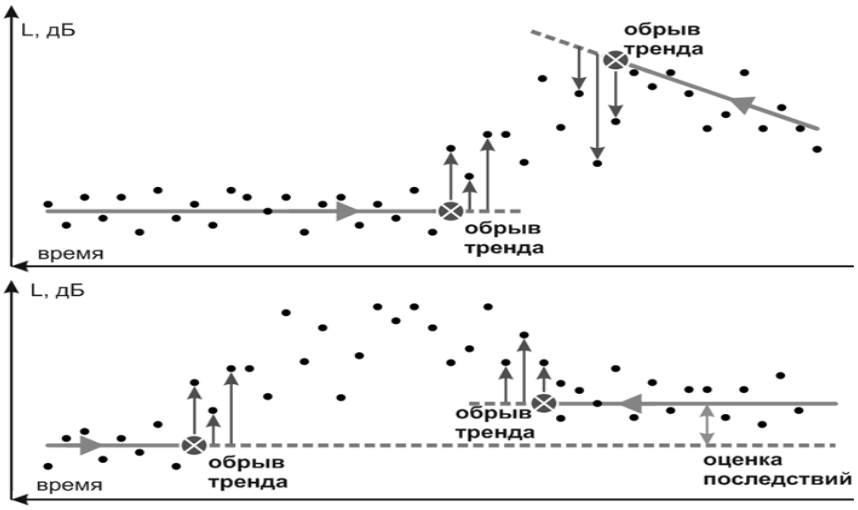


Рис. 3. Пример анализа данных в накопителе на 64 измерения. Сверху – типовая картина распределения данных при входе в опасный режим и приработке, снизу – завершение приработки, стабилизация.

Для выделения данных компонент отвечает отдельный модуль системы, особенностью которого является анализ трех последовательных спектров без усреднения – см. рис. 4, что позволяет идентифицировать гармонические ряды при повышенной нестабильности, в то время как при усреднении спектров в этом случае гармоники начинают разваливаться. При выбранном подходе разброс фона (случайных составляющих) гораздо сильнее, чем в усредненном спектре, что потребовало создания новых алгоритмов автоматической идентификации гармонических рядов при высоком уровне помех. Модуль позволяет идентифицировать пять гармонических рядов по 6 гармоник, как при наличии данных с датчика оборотов, так и при их отсутствии, в этом случае данных ряды ищутся в заданных широких интервалах.

Выходными данными системы является информация о состоянии контролируемых агрегатов в виде светофоров на мнемосхеме, а также списки дефектов и рекомендации по обслуживанию. Также предусмотрено получение дополнительной информации в виде графического отображения выбранного параметра в виде данных в указанном накопителе (при этом отображаются пороги и тренды).

В отличие от классических систем виброконтроля и мониторинга разработанная система отличается значительным повышением достоверности определения опасных состояний, а также возможностью контроля в переходных режимах, в которых чаще всего и происходят аварии. Также система имеет ряд полезных функций – таких как определение времени наработки для каждого агрегата и записи первичных сигналов для глубокого экспертного анализа.

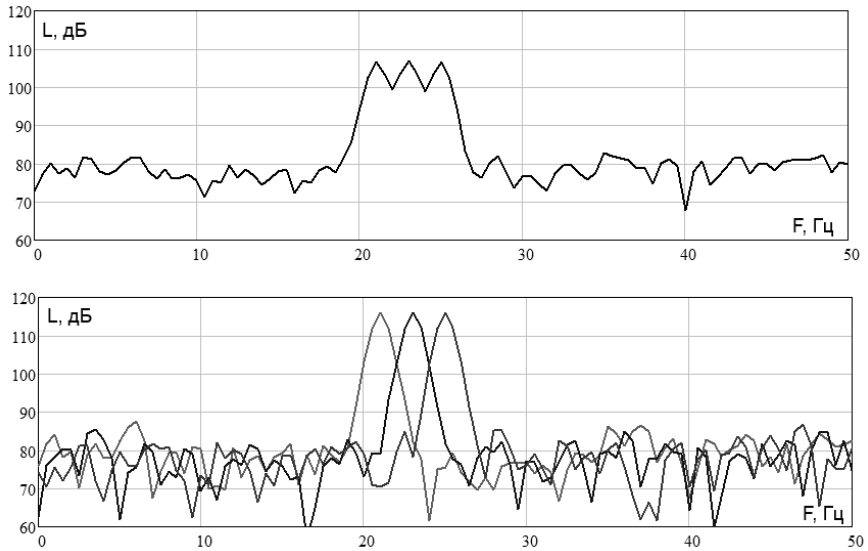


Рис. 4. Усредненный спектр (сверху) и три мгновенных спектра (снизу) при высокой нестабильности частоты.

Используемые в системе алгоритмы диагностики отрабатывались на многих типах машин, как общего применения, в энергетике и на железнодорожном транспорте, так и судовых, в частности на газовых и паровых турбинах, планетарных редукторах, турбогенераторах, центробежных и осевых насосах, в том числе погружных. Первые образцы разработанной системы оперативного диагностирования используются на морском транспорте и в составе автономной электроэнергетической установки с газотурбинным приводом.

СПИСОК ЛИТЕРАТУРЫ

1. Неразрушающий контроль: Справочник: В 7т. Под общей редакцией В.В. Клюева. Т. 7: В 2 кн. Кн. 2: Ф.Я. Балицкий, А.В. Барков, Н.А. Баркова и др. Вибродиагностика, – М.: Машиностроение, 2005, 829 с.
2. Барков А.В., Баркова Н.А., Грищенко Д.В., Федорищев В.В. Система мониторинга вибрации с оперативной идентификацией обнаруживаемых изменений. Сборник докладов Всероссийской научно-практической конференции с международным участием «Защита от повышенного шума и вибрации». – СПб.: 2013, 743 с.
3. Барков А.В., Баркова Н.А., Грищенко Д.В. Бортовая система диагностики судовых машин. Сборник тезисов докладов первой научно-практической конференции «Современные технологии автоматизации борьбы за живучесть». – СПб, 2012, 83 с.
4. Барков А.В. Бортовые системы мониторинга и оперативной диагностики вращающегося оборудования. Научно-технический обзор. URL: http://vibro-expert.ru/bortovie-sistemi-monitoringa-i-operativnoie-diagnostiki-vrashayushegosya-oborudovaniya.html (дата обращения: 25.08.2014).

УДК 004.42

ПРОГРАММНАЯ ОБОЛОЧКА РАСПАРАЛЛЕЛИВАНИЯ ДЛЯ ВОССТАНОВЛЕНИЯ ДОСТУПА К ДАННЫМ

Егоров Александр Николаевич[1], Кузнецов Виталий Александрович[1], Назаргулов Ильшат Азатович[2],
[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, дом 5/7,
[2] ООО «Специальный технологический центр»,
Россия, Санкт-Петербург, ул. Гжатская, д.21,
e-mails: eanspb@rambler.ru, ky3bma.92@mail.ru, nazargulov.i@gmail.com

Аннотация: В статье рассмотрены модель и особенности реализации программной оболочки распараллеливания. Приведены результаты сравнительной оценки производительности решения задачи восстановления доступа к данным на различных аппаратных средствах, используя для этих целей, как последовательный алгоритм вычисления, так и реализацию на основе программной оболочки распараллеливания.

Ключевые слова*: параллельные алгоритмы; технология CUDA*

PROGRAM SHELL OF PARALLELIZING FOR RESTORATION OF ACCESS TO DATA

Alexander Yegorov[1], Vitali Kuznetsov[1], Ilshat Nazargulov[2],
[1] Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
[2] Special Technology Center,
Russia, St. Petersburg, Gzhatskaya str. 21,
e-mails: eanspb@rambler.ru, ky3bma.92@mail.ru, nazargulov.i@gmail.com

Abstract: In article the model and implementation feature of the program shell of parallelizing are considered. Results of the comparative performance evaluation of solving the task of access restoring to data on a various hardware, using for these purposes, both a sequential algorithm of computing, and implementation on the basis of the program shell of parallelizing are given.

Keywords: *parallel algorithms; CUDA technology*

Введение. 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 этой 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.

Одним из возможных методов решения этой задачи является перебор возможных ключей. Метод, с одной стороны, надёжен, поскольку его использование всегда гарантирует получение результата, но с другой стороны, требует больших временных затрат, в связи с выполнением огромного количества однородных операций. Для снятия указанной проблемы при автоматическом восстановлении секретного ключа воспользуемся механизмом распараллеливания вычислительного процесса, который реализован в виде программной оболочки распараллеливания (ПОР).

Модель ПОР. Основная цель программного обеспечения – получить задачу от пользователя и вернуть ему результат. Для решения пользовательских задач используются вычислительные мощности устройств компьютера. Для этого ПОР обеспечивает взаимодействие ресурсов компьютера.

ПОР представляет собой совокупность взаимодействующих модулей. Связующим звеном этих модулей является ядро программной оболочки (ЯПО). ЯПО включает в себя базовую функциональность ПОР, имеет самую высокую независимость от других модулей. Вся основная логика работы ПОР заложена во взаимодействии ЯПО с модулями устройств. Модули устройств (МУ) выполняют основную работу вычислений ПОР – решение пользовательских задач (ПЗ). Предполагается также, что МУ имеют одно из двух состояний: busy (устройство занято) и free (устройство свободно).

При формировании требований к параллельным алгоритмам наиболее важным является определение последовательности выполнения определённых событий для каждого вычисления программы. Таким образом, для описания модели ПОР достаточно использовать язык темпоральной логики линейного времени (LTL), в котором явно учтен феномен времени. Каждое событие будет характеризоваться булевой переменной, которая принимает значение «Истина» тогда и только тогда, когда наступает событие.

Для описания модели введем следующие атомарные высказывания, соответствующие основным событиям вычислений программы:

- tryi – i-ый пользователь собирается отправить задачу;
- addi – i-ая ПЗ добавляется в очередь задач;
- deli – i-ая ПЗ удаляется из очереди задач;
- sendi – i-ая ПЗ отправляется задачи на решение в МУ;
- createi – i-ая подзадача формируется из ПЗ;
- solvei – i-ый МУ решил подзадачу;
- recvi – i-ый результат подзадачи МУ отправляется ЯПО;
- resi – формируется i-ый результат ПЗ;
- free – МУ свободен;
- busy – МУ занят;
- end – получен конечный результат ПЗ;
- empty – очередь задач пуста.

Рассмотрим математическую модель программной оболочки построенную на основе языка LTL:

1. Всякий раз, когда пользователь собирается запустить ПЗ, ЯПО добавляет себе ПЗ в очередь задач:

$$G(try_i \rightarrow add_j); \quad (1)$$

2. Пока очередь задач не окажется пустой (empty), ЯПО будет отправлять задачи на решение свободным МУ (free):

$$G((free \rightarrow send_j)\ U\ emplty); \quad (2)$$

3. всякий раз, когда ЯПО отправляет задачу МУ, формируется подзадача для этого модуля:

$$G(send_i \wedge X\ create_i); \quad (3)$$

4. всякий раз, когда у МУ формируется подзадача, он становится занятым (busy):

$$G(create_j \rightarrow busy); \quad (4)$$

5. всякий раз, когда МУ становится занятым, должна когда-нибудь решиться подзадача:

$$G(busy \rightarrow F\ solve_i); \quad (5)$$

6. после решения подзадачи МУ возвращает результат ЯПО, и становиться свободным (free):

$$G(solve_i \rightarrow X(recv_j \wedge free)); \quad (6)$$

7. всякий раз, когда ЯПО получает результат решения подзадачи от МУ, ЯПО формирует результат соответствующей ПЗ:

$$G(recv_i \rightarrow X\ res_j); \quad (7)$$

8. всякий раз, когда ЯПО формирует результат решения ПЗ, оболочка проверяет, получен или нет конечный результат. Если этот результат получен, то ПЗ удаляется и очереди:

$$G((res_i \wedge end) \wedge del_j). \quad (8)$$

Полученные зависимости темпоральной логики позволяют представить псевдокод основных процессов модели ПОР (таблицы 1, 2). Для каждой операции псевдокода ставится счетчик, который логически делится на два поля: <номер потока>.<номер счётчика в потоке>. Следует заметить, что псевдокод МУ является инвариантным по отношению ко всем вычислительным устройствам.

Далее в соответствии построенному псевдокоду строится размеченная система переходов LTS (Labelled Transition System), где учитываются всевозможные состояния ПОР.

Основными состояниями ПОР являются:

– счетчики выполнения команд;
– состояние модуля устройства (занят/свободен);
– состояние решения задачи (решено/не решено).

На рис. 1. изображены схемы LTS для каждого отдельного потока: для единственного потока ЯПО и для множества потоков МУ. В узлах через запятую показаны значения основных состояний ПОР.

Программная реализация. Программная реализация оболочки предназначена для распараллеливания процесса вычислений в прикладных решениях, используя для этих целей центральный процессор и графическую видеокарту, которая поддерживает технологию CUDA компании NVIDIA. CUDA – это платформа параллельных вычислений и модель программирования, позволяющая существенно увеличить вычислительную производительность за счёт максимально эффективного использования ресурсов видеокарты (графических процессоров и памяти) компании NVIDIA.

Таблица 1

Псевдокод ЯПО модели ПОР

Счётчик	Псевдокод
	while (true)
	{
1.1.	if (try)
1.2.	add(task);
1.3.	while (!empty && status == free)
1.4.	send(task);
1.5.	if (recv(subtask))
	{
1.6.	res(subtask);
1.7.	if (end)
1.8.	del(task);
	}
	}

Поддержка прикладных решений реализуется в виде dll библиотек, разработанных для каждого типа устройства с которыми работает ПОР. Каждая библиотека должна реализовать ряд экспортных функций обеспечивающих выполнение следующих операций:

– вычисление оценки производительности устройства;
– проверку, обработку и формирование данных пользовательской задачи (ПЗ);
– декомпозицию задачи на подзадачи;
– решение подзадач;
– формирования общего результата ПЗ.

В рамках проблемы восстановления доступа к данным были созданы библиотеки для восстановления секретного ключа алгоритма шифрования DES. При реализации библиотек для отладки параллельных алгоритмов использовался NVIDIA Nsight позволяющий оптимизировать производительность вычислений, как для центрального, так и для графических процессоров.

Таблица 2

Псевдокод МУ модели ПОР

Счётчик	Псевдокод
	while (true)
	{
2.1.	if (subtask = create(task))
	{
2.2.	status = busy;
2.3.	while (solve(subtask)) {}
2.4.	recv(subtask);
2.5.	status = free;
	}
	}

Количественная оценка производительности решения задачи восстановления ключа алгоритма шифрования DES в разработанной среде ПОР с применением технологий CUDA представлена в таблице 3. Значения таблицы, показывают эффективность применения ПОР для восстановления доступа к данным.

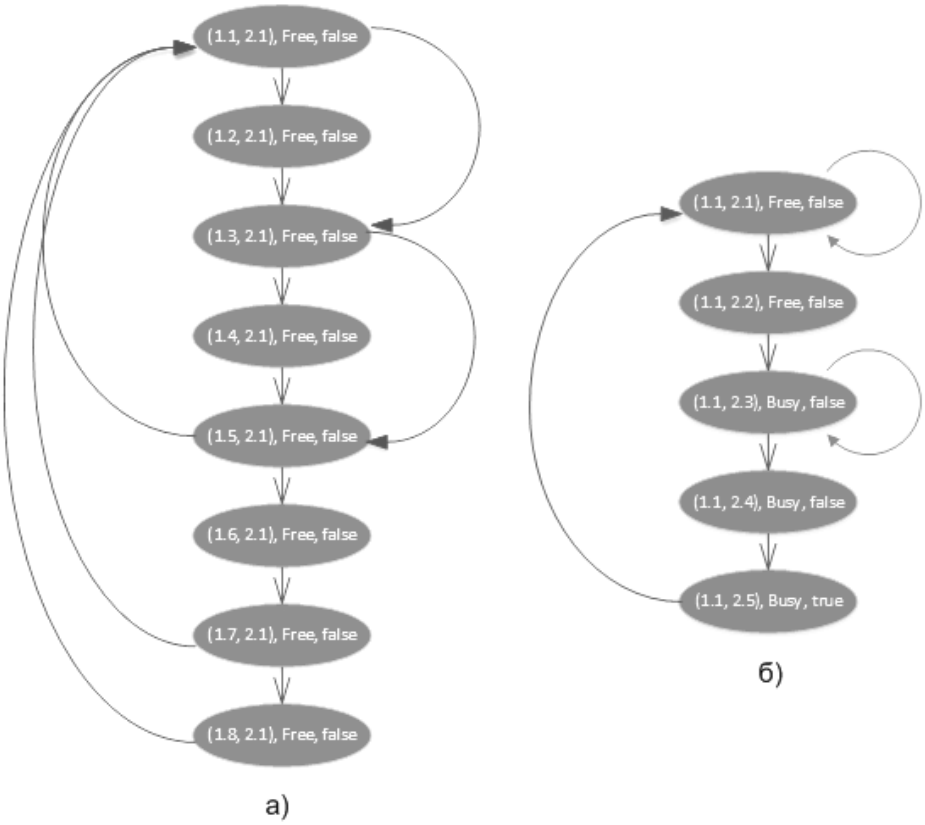


Рис. 1. LTS потоков ПОР: а) - ЯПО; б) - МУ

Таблица 3

Результаты оценки производительности решения задачи по восстановлению ключа алгоритма шифрования DES на конкретных вычислительных устройствах

Устройство	Режим решения		
	Последовательный (ключей/сек)	Параллельный на основе ПОР (ключей/сек)	Параллельный на основе ПОР с применением технологии CUDA (ключей/сек)
Процессор Intel core i5	~160 000	~15 000 000	
Процессор Intel core i7	~200 000	~20 000 000	
Видеокарта NVIDIA GTX 256			~156 000 000
Видеокарта NVIDIA GTX 590			~1 000 000 000

Заключение. Разработанный подход решения ПЗ в интегрированной программной среде оболочки распараллеливания можно считать универсальным. Это означает, что практически любую задачу пользователя, требующую для повышения производительности использования распараллеливания вычислений, можно решить в этой программной среде, реализовав необходимые библиотеки. ПОР является автоматизированной программной системой, которая использует весь потенциал подключенных к компьютеру вычислительных устройств, допускающих распараллеливание.

СПИСОК ЛИТЕРАТУРЫ

1. Боресков А.В. и др. Параллельные вычисления на GPU. Архитектура и программная модель CUDA: Учебное пособие. – М.: МГУ, 2012, 336с.
2. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программных систем. – Спб.: БХВ-Петербург, 2010, 560с.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – Спб.: БХВ-Петербург, 2009, 576с.

УДК 004.7

О НЕКОТОРЫХ МЕТОДАХ ИСПОЛЬЗОВАНИЯ МОДЕЛЕЙ ПЕРКОЛЯЦИИ ДЛЯ МОДЕЛИРОВАНИЯ ПРОЦЕССА В ИНФОРМАЦИОННЫХ СЕТЯХ

Некрасова Анна Алексеевна, Соколов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7
e-mails: anna14_06@mail.ru, sssokolov@mail.ru

Аннотация. Проведен обзор использования перколяционных моделей в информационных сетях. Перколяционная модель представляет собой распространение процесса на решетке, при котором существует хотя бы один непрерывный путь через соседние проводящие узлы от одного до противоположного края.

Ключевые слова: *перколяция, статистическое моделирование, информационные сети, перколяционная лавина, эффект перколяции.*

SOME METHODS OF USING THE MODEL OF PERCOLATION PROCESS MODELING IN INFORMATION NETWORKS

Anna A. Nekrasova, Sergey S. SokolState University of Marine and River Fleet Admiral Makarov,
Russia, St. Petersburg, ul. Dvina, 5/7
e-mails: anna14_06@mail.ru, sssokolov@mail.ru

Abstract. An overview of the use of percolation models in information networks. The percolation model is an extension of the process on the grid, in which there is at least one continuous path through the adjacent conductive components from one to the opposite edge.

Keywords: *percolation, statistical modeling, information networks, percolation avalanche effect percolation.*

Введение. На сегодняшний день очень быстро развиваются информационные технологии. На ряду с этим увеличивается количество проблем, которые необходимо решать в ходе возникновения. Существуют методы решения этих проблем: имитационное моделирование, линейное программирование, метод теории вероятностей, метод теории игр и т.д. В данной статье мы будем говорить о перколяционных моделях. Их использование позволяет решить проблемы в информационных сетях.

Сегодня перколяционные модели, как и в прочем теория перколяции, не сильно распространены в решении информационных задач. Но существует ряд работ посвященных внедрению методов перколяции для сетевых алгоритмов. Например, лавинная маршрутизация на основе перколяции для сенсорных сетей [1]. Предлагается уменьшать вероятность пересылки сообщения по мере удаления от источника. Тем самым резко уменьшается число копий сообщений, а вероятность достижения адресата падает незначительно. Перколяционная маршрутизация для оптической кластерной сети источни [1]. Здесь эффект перколяции используется для предотвращения образования «узких мест» в коммуникационной сети, связывающей узлы кластера (в качестве топологии кластера рассматривается 3D–решетка). Перколяционный поиск в сетях со степенным распределением связности [1]. Здесь предлагается алгоритм поиска для пиринговых сетей, использующий встречные процессы внедрения и запроса контента и основанный на свойстве «накопления» информации в «ключевых» узлах с большой степенью связности.

В информационных сетях используется дискретный вариант перколяционных моделей. Частицы среды представляются как вершины графа, имеющие два состояния: «проводящее» и «непроводящее». Смежными считаются соседние вершины, находящиеся в проводящем состоянии.

Назначение состояний вершинам происходит в случайном порядке, но с одинаковой вероятностью p. В такой постановке порог перколяции – это значение вероятности p*, при котором в графе образуется «перколяционный кластер» – т.е. связная область, обеспечивающая протекание (жидкости, тока и т.п.) через среду [1].

Если рассматривать вопрос сокращения расходов на рассылку данных в динамических сетях (сети с неустойчивыми связями) за счет использования механизма «Перколяционной лавины», будет видно соотношение между порогом перколяции в классическом (статическом) и динамическом случаях через интегральную статистическую характеристику:

1) переход от отсутствия протекания к полному протеканию происходит на сравнительно узком интервале, что в целом аналогично классическому случаю;

2) в отличие от классической ситуации формирования «бесконечного» кластера (или кластера от стенки до стенки) формируется динамический связывающий кластер, который изменяется, но при этом в любой момент времени обеспечивает связь левой и правой стенок;

3) значения порога перколяции в динамическом и статическом случаях взаимосвязаны через интегральную статистическую величину, характеризующую временные параметры связей (средняя вероятность активности связи);

4) перколяционная лавина особенно эффективна по затратам (сокращение расходов до 2.5 раз) в случае большой связности.

Таким образом, перколяционная лавина может найти свое применение в высокодинамичных мобильных сетях, уровень изменений топологии в которых настолько высок, что лавинная доставка данных является единственным способом маршрутизации. В этом случае перколяционная лавина обеспечивает тот же уровень доставки данных что и обычная, экономя при этом трафик [1].

Следующий подход к исследованию больших сетей связан с моделью перколяции по их ребрам информационного и транспортного трафика. Управляемая перколяция зоны обслуживания реализуется в две фазы: на первой создается стохастическая основа с относительно небольшой концентрацией объектов, не обеспечивающей стохастическую перколяцию, а на второй в межкластерные интервалы вводятся дополнительные объекты с целью получения кратчайшего перколяционного пути через стохастическую основу при сравнительно низком общем количестве объектов и минимизации общих затрат [2]. Большие (сложные) сети характеризуются большим числом узлов, топологией и свойствами каждого узла. Из них выходят исследования их совокупных свойств и ряд вытекающих из них статистических феноменов в частности: – статистические характеристики случайных операционных сред, образованных сетью, – пути, проложенные в сетях по выбранным критериям качества, – образование кластеров узлов (объектов), связанных по определенным условиям, – статистические распределения узлов, связей, кластеров и трафиков [2]. Один из развиваемых подходов к исследованию больших сетей связан с моделью «протекания» по их ребрам информационного трафика, безопасного информационного трафика, транспортного трафика, потоков обслуживания и т.п. Теория перколяции решает задачи анализа больших сетей в рамках этой модели. Название возникло в связи с тем, что ряд первых работ в этом направлении был посвящен процессам просачивания (протекания) жидкостей или газов через случайную пористую среду [3–4].

Постановка задачи теории перколяции следующая: имеется решетка из связей или матрица, случайная часть ячеек которых K – «черная», проводящая поток, а остальная часть – «белая», не проводящая поток. Необходимо найти минимальную концентрацию «черных» ячеек, при которой имеется сквозной путь по черным связям через всю матрицу в заданном направлении, иными словами, такую концентрацию Kn, при которой вся матрица в целом проводит. При достижении проводимости свойства такой сети качественно и скачком меняются: образуется безопасный путь (или он разрушается), возникает (или затухает) эпидемия, воссоздается разрушенная социальная сеть, возникает пробка в дорожном движении и т.п. Концентрация K – это доля черных узлов при случайно-однородном заполнении решетки или матрицы является вероятностью наличия черного объекта в ячейке матрицы [5].

Статистическое моделирование на таких случайных матрицах позволяет обнаружить и исследовать статистический феномен порога перколяции как «пробоя» матрицы проводящим перколяционным кластером при достижении вероятности нахождения объекта в ячейке значения Kn [**]. Теория перколяции позволяет определить порог перколяции, уровень вероятности или концентрации Kn, при которой наступает перколяция, и имеет много точных аналитических результатов, но основной используемый ею метод – численное статистическое моделирование на решетках или деревьях. Большинство прикладных задач анализа и исчисления путей в больших сетях связаны с минимизацией длины пути – числа узлов сети, входящих в искомый маршрут. В рассмотренном случае стохастической перколяции искомый путь получается случайным образом при повышении концентрации объектов с заданными свойствами в сети. Дальнейшего снижения потребной концентрации объектов и, следовательно, необходимого их количества для реализации перколяции зоны обслуживания сети можно достичь, если сначала создать опорную систему распределенных случайным образом объектов при сравнительно малой их концентрации, а затем на втором этапе операции в межкластерные интервалы «стохастической опоры» ввести управляемым

образом ограниченное количество дополнительных объектов так, чтобы они совместно с имеющимися стохастическими кластерами образовали бы сплошной перколяционный путь минимальной длины в заданном направлении. Таким образом, увеличивая концентрацию объектов в стохастической основе большой сети, можно уменьшить необходимое для создания кратчайшего перколяционного пути число дополнительных управляемых объектов и наоборот [2].

Если необходимо найти в ячейке объект, и значение вероятности нахождения соответствуют порогу перколяции, то на оси вероятности нахождения этого объекта в ячейке будет иметься другая точка – точка максимальной кластеризации. Среднее число кластеров по матрице максимальное. При добавлении новых объектов, идет активное присоединение к уже образованным кластерам, но происходит слияние класстеров со снижением их общего количества.

Имеется две фазы операции на больших сетях. Первая фаза. В ней создается стохастическая основа с концентрацией случайных распределенных объектов значительно меньшей порога стохастической перколяции [2]. Вторая фаза. Через кластеры стохастической основы, которые уже имеются, проводится кратчайший перколяционный путь, добавляя межкластерные интервалы дополнительных «управляемых» объектов. Таким образом, статистические феномены образования случайных кластеров при статистическом моделировании больших сетей на матрицах, обеспечивают минимум суммарных затрат оценки суммарной эффективности двухфазной операций на больших сетях и значений концентрации объектов. Следующий метод – это двухуровневый метод декомпозиции графа, описывающего перколяционную решетку, который позволяет выполнить балансировку загрузки вычислительных узлов [6]. Расчетную сетку необходимо разбить на большое число компактных блоков – микродоменов, каждому из которых будет принадлежать некоторое количество узлов сетки, а макрограф будет описывать топологию сетки блоков. Каждая из вершин макрографа представляет собой микродомен, а ребро — связь между ними. Вершины имеют веса, равные количеству узлов в микродоменах. Балансировка в этом случае достигается при разбиении макрографа на части по числу процессоров. Особенностями алгоритма обусловлены дополнительные требования к разбиению:

1) параллелепипеды, описанные вокруг вершин микродоменов, не должны иметь пересечений;

2) заполнение параллелепипедов узлами должно быть максимально плотным (расчет узлов внутри параллелепипеда осуществляется независимо от того, активен узел или нет);

3) параллелепипеды не должны быть слишком малых размеров;

Заключение. Хочется отметить, что эффект перколяции в информационных сетях не часто наблюдается в решении той или иной информационной задачи, но и применение математических методов с пересечением перколяционных моделей несет за собой интересные исследования, позволяющие находить эффективные решения. Использование перколяционных моделей дает возможность значительно сократить объем вычислений и расчетов.

СПИСОК ЛИТЕРАТУРЫ

1. Голубев А.С., Звягин М.Ю., Милованов Д.С. Эффект перколяции в информационных сетях с неустойчивыми связями, 2011 г.
2. Мостовой Я.А. Управляемая перколяция в больших сетях, 2013 г.
3. Тарасевич, Ю.Ю. Перколяция: теория, приложения, алгоритмы. М.: УРСС, 2002. – 109с.
4. Тарасевич Ю.Ю. Математическое и компьютерное моделирование. М: Едиториал УРСС, 2003. – 144с.
5. Москалев П.В., Шимтов В.В. Математическое моделирование пористых структур. М: Физматлит, 2007. – 120с.
6. Воронюк М.Н. Математическое моделирование процессов фильтрации в перколяционных решетках с использованием вычислительных систем сверхвысокой производительности, 2013 г.
7. Abalakin I. V., Boldyrev S. N., Chetverushkin B. N., Zhokhova A. V., Iakobovski M. V. Parallel algorithm for solving flow problems on unstructured meshes // Proc. of 16th IMACS World Congress. Lausanne, Switzerland, Aug. 21— 25, 2000.
8. NVIDIA. CUDA C Programming Guide. 2012. Vol. 5.0.
9. S. Dasgupta, C.H. Papadimitriou, and U.V. Vazirani «Algorithms», 2006

УДК 623.9, 623.618, 629.585

СЕТЕВОЕ ПЛАНИРОВАНИЕ И УПРАВЛЕНИЕ ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СУДАМИ И БОРЬБОЙ ЗА ЖИВУЧЕСТЬ

Поленин Владимир Иванович, Ребенóк Юрий Станиславович
Военный учебно-научный центр ВМФ «Военно-морская академия»
Россия, Санкт-Петербург, Ушаковская наб., 17/1
e-mail: polenin@mail.ru

Аннотация: В статье рассматривается проблема повышения эффективности автоматизированных систем управления судами и борьбой за живучесть. Решение проблемы достигается составлением сценария текущего управления судном в нормальном режиме эксплуатации и в условиях возникновения аварийных повреждений, с реализацией этого сценария с помощью аппарата сетевого

планирования и управления на основе информационной технологии сетевого общего логико-вероятностного метода (ОЛВМ). Приводятся основные положения сетевого планирования и управления и демонстрационный пример их реализации.

Ключевые слова: *планирование; управление; сетевые методы; автоматизированные системы; борьба за живучесть; морские суда.*

NETWORK PLANNING AND MANAGEMENT THE PERSPECTIVE DIRECTION OF PERFECTION OF THE AUTOMATED CONTROL SYSTEMS OF COURTS AND STRUGGLE FOR SURVIVABILITY

Polenin Vladimir, Rebenok Yury
Military uchebno-centre of science of Navy "Naval academy"
Russia, St.-Petersburg, Ushakovsky emb., 17/1
e-mail: polenin@mail.ru

Abstract: In article the problem of increase of efficiency of the automated control systems by courts and struggle against failures, fires and for survivability is considered. The solution of a problem is reached by drawing up of the scenario of current management by a vessel in a normal mode of operation and in the conditions of occurrence of emergency damages, with realisation of this scenario by means of the device of network planning and management on the basis of information technology of a network general logiko-likelihood method. Substantive provisions of network planning and management and a demonstration example of their realisation are resulted.

Keywords: *planning; management; network methods; the automated systems; struggle for survivability; sea-crafts.*

Введение.

По мере развития автоматизированных систем разных поколений, поддерживающих управление, собственно управления изменился мало. Это по-прежнему сквозное управление на протяжении периода времени выполнения текущих задач грузовых работ, рейсов, ремонтно-профилактических работ, и это – циклический процесс циклической реализации сквозного сценария с периодом от несколько минут, назначаемым ЛПР, до регламентных 4, 8, 12 и 24 часов.

Как бы ни были совершенно СМО и дружественен интерфейс АСУ, они процесс управления в полной мере не обеспечивают. Решается заданный набор задач наблюдения, навигации, управления движением, силовой установкой, но не решается задача организации и поддержки управления в целом. Причем система управления борьбой с авариями, пожарами и за живучесть (непотопляемость) создается отдельно. Объединение этих систем путем их комплексирования обычно предусматривается, но функционируют они практически независимо одна от другой.

1. Сетевое планирование и управление в АСУ

В последнее время актуальной стала проблема перехода от создания комплексированных АСУ к созданию интегрированных АСУ. Комплексирование имеет три аспекта: аппаратурный, или технический, программный и информационный. Но как бы не было тесным комплексирование, в том числе по повседневному и аварийному управлению, оно комплексированием и остается, не перерастая в интегрированное. Остается до того, пока автоматизация не обеспечит организацию и поддержку основного процесса системы − собственно управления во всех его аспектах одновременно.

Для интеграции процесса управления необходимо составить сценарий его выполнения и описать в нем операции выполнения частных задач, взаимодействия всех частных систем между собой на пути к достижению главной цели выполняемых задач в повседневных и аварийных условиях.

Спрашивается, какая информационная технология способна обеспечить реализацию такого управляющего сценария? Здесь нужно подобрать синоним понятию управляющего сценария. Таким синонимом является известное понятие сетевого планирования и управления.

Пока в автоматизированных системах управления сетевые планы получили развитие и применение лишь в виде мнемосхем. Задачи управления процессами, реализуемые с применением мнемосхем, специфически ограничены областью только детерминированных моделей технических систем с фиксированной структурой, относительно немногочисленной по элементам и простой по их взаимосвязям.

Полноценная реализация сетевого планирования и управления на большой, сложной и динамической сети требует создания компьютерной информационной технологии сетевого планирования и управления в темпе текущего времени.

Сегодня такие технологии имеются. Сетевое планирование и управление наиболее доступно реализуется с применением информационной технологии Сетевых ОЛВМ и ОЛДМ [1] на основе

комплексов ПК АСМ 2011 и ПК «АРБИТР» ОАО «СПИК СЗМА» [2] путем их встраивания в АСУ и адаптации к модели задач управления коллективной деятельностью.

2. Пример реализации

Рассматривается функционирование топливного трубопровода в агрессивной (опасной) среде. Наличие опасности аварийного развития событий – стандартная характеристика опасных производственных объектов (ОПО).

Ориентированный граф аварийного развития событий в форме схемы функциональной целостности (СФЦ) [1] приведен на рис. 1.

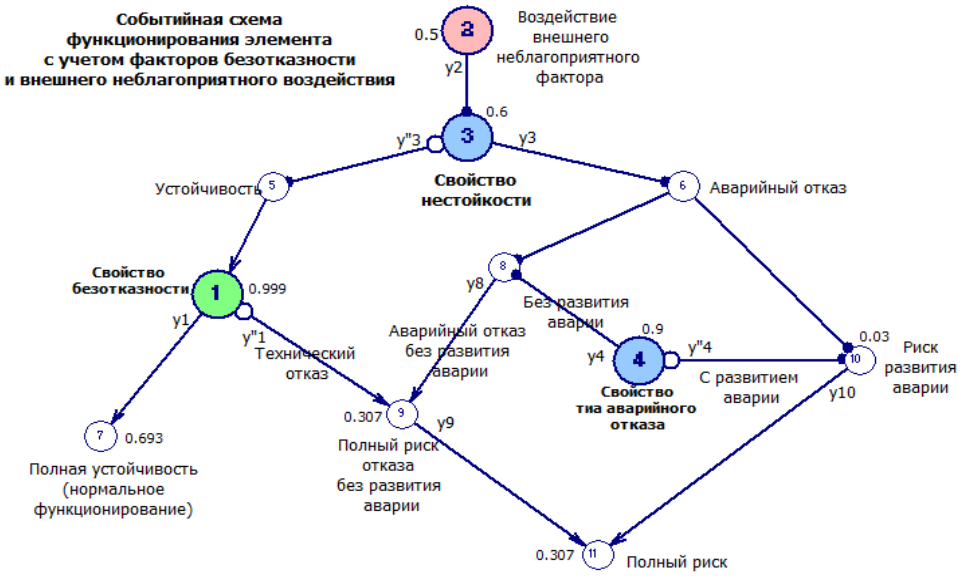


Рис. 1. СФЦ функционирования элемента технической системы с комбинированным учетом влияющих факторов

Ориентированный граф аварийного развития событий в форме схемы функциональной целостности (СФЦ) [1] приведен на рис. 1.

Пусть y2 – событие воздействия, по каким-либо причинам, по трубопроводу внешнего неблагоприятного фактора, например, ударное. Вероятность его появления, как вероятность неблагоприятного стечения обстоятельств, считаем известной, она определяется расчетным путем по условиям функционирования элемента (P2=0.5).

Трубопровод характеризуется определенной и известной стойкостью к этому воздействию с вероятностью Pc. Вероятность нестойкости 1Pc=0.6.

При проявлении свойства стойкости y3 с вероятностью P(y3)=0.4 наступает событие 5 устойчивости элемента к воздействию внешнего неблагоприятного фактора. Далее, при проявлении свойства безотказности 1, наступает событие или состояние 7 полной устойчивости элемента, т. е. его нормального функционирования.

Если проявляется свойство нестойкости (y3) трубопровода к воздействию внешнего неблагоприятного фактора, то могут иметь место два исхода, представленных вершиной-событием 4:

– исход-событие y4 повреждения и отказа трубопровода без развития аварии, например, при таком типичном следствии удара по трубопроводу, как его смятие и, вследствие этого, утрата транспортной пропускной способности;

– исход-событие y4 повреждения и отказа трубопровода с аварией, например, вследствие разрушения оболочки трубопровода.

Произведение в вершине (8) событий (y3) нестойкости трубопровода к удару и (y4) смятия оболочки трубопровода с утратой транспортной пропускной способности, представляет собой наступление события (y8) аварийного отказа трубопровода без развития аварии.

Произведение в вершине (10) событий (y3) нестойкости трубопровода к удару и (y4) разрушения оболочки трубопровода с развитием аварии, представляет собой наступление события (y8) аварийного отказа трубопровода с развитием аварии.

Смятие и разрушение оболочки трубопровода как следствия его нестойкости к удару, могут быть изучены и оценены в вероятностной мере, например, по потенциальной частости их наступления в эксперименте или по соотношению показателей устойчивости к смятию и разрушению, полученных методами теории сопротивления материалов.

Пусть смятие и разрушение оболочки трубопровода наступают в соотношении 9:1, тогда выходам вершины 4 соответствуют вероятности P(y4)=0.9 и P(y4)=0.1.

Свойства-события 3 нестойкость трубопровода к удару, как условие возникновения

повреждения трубопровода, и 4 характер повреждения, являются независимыми между собой. Соответственно, вероятности наступления событий у4 могут рассматриваться как условные. Тогда вероятности наступления событий у8 аварийного отказа трубопровода без развития аварии и у10 аварийного отказа трубопровода с развитием аварии будут представлять собой произведения этих вероятностей:

$$P_8 = P_3 P_4;\ P_{10} = P_3\left(1 - P_4\right). \quad (1)$$

Далее, событие (у8) отказа без развития аварии и эксплуатационный отказ (у 1) трубопровода по физическому смыслу однородны и потому могут быть объединены в вершине-событии 9, характеризующей полный риск отказа без развития аварии.

Наконец, сочетание полного риска отказа без развития аварии (у9) и риска развития аварии (у10) приводят к понятию полного риска (у11).

Следует обратить внимание на то обстоятельство, что полученные значения вероятностей полного риска отказа без развития аварии Р(у9) и полного риска Р(у11) практически равны между собой (0.307). Это обусловлено традиционно высокой надежностью элементов структурно-сложных систем. С учетом данного обстоятельства живучесть структурно-сложных систем принято рассматривать как свойство сохранять работоспособность при случайных поражениях элементов вследствие воздействия поражающих факторов (ударов, взрывов, пожаров и т.п.) в предположении об абсолютной надежности элементов системы.

3. Пример формирования СФЦ структурно-сложного объекта с помощью модульной схемы функционирования элемента технической системы с комбинированным учетом влияющих факторов

Ниже приводится пример части схемы системы выгрузки ГСМ из танков (рис. 2). Требуется составить СФЦ этой системы с помощью рассмотренной выше модульной схемы функционирования элемента технической системы.

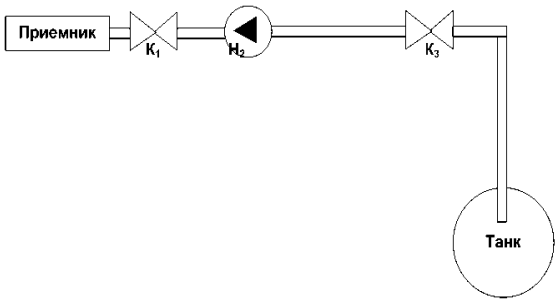


Рис. 2. Схема системы выгрузки ГСМ из танков

Система состоит из танка, трубопровода, насоса, двух клапанов и приемника ГСМ.

Используя модульную СФЦ (рис. 1) последовательно для всех элементов системы, получим СФЦ функционирования системы в целом (рис. 3).

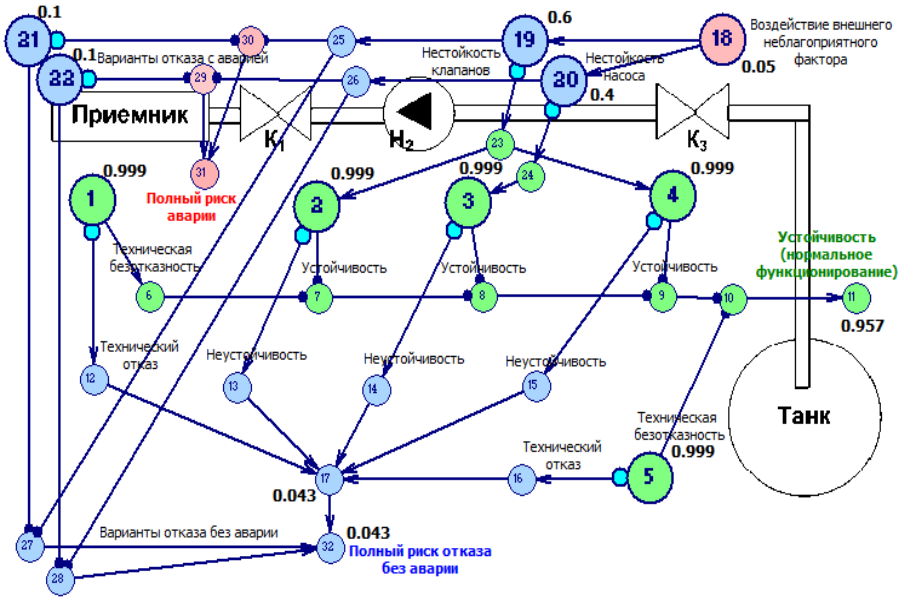


Рис. 3. СФЦ системы выгрузки ГСМ из танков

Нестойкости к внешнему неблагоприятному фактору приняты различными для клапанов и насоса.

Этим демонстрируется возможность индивидуального или группового подхода к учету каждого из влияющих факторов по всем элементам структурно-сложной системы. Достоверность итоговой СФЦ и результатов моделирования подтверждается выполнением условия нормировки, а именно, равенства единице суммы показателей устойчивости (вершина 11) и полного риска (вершина 17).

Выводы

1. Решена одна из важных задач системного анализа структурно-сложных объектов задача создания модульных структурных схем функционирования элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в форме сетей планирования и управления. Результаты решения задачи ориентированы на информационную технологию ОЛВМ, реализованную в программном комплексе «АРБИТР» [2].

2. Разработана структурная схема функционирования элементов, которая комбинированно отражает влияние одновременно всех основных обычно учитываемых факторов и свойств и позволяет вычислять системные характеристики систем одновременно по всем основным обычно интересующим показателям. Решена задача стандартизации, как приведения к единой системе эталонов, и унификации, как приведения эталонов к минимальному числу типовых форм.

3. Полученные результаты обеспечивают реализацию принципа доступности методов и технологии сетевого ОЛВМ для широкого круга пользователей и способствуют объективизации системных исследований структурно-сложных систем и опасных производственных объектов.

СПИСОК ЛИТЕРАТУРЫ

1. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства Свирин, И.А. Гладкова. Под ред. А.С. Можаева // Проект в рамках Концепции социально-политического проекта РАЕН «Актуальные проблемы безопасности социума» / Российская академия естественных наук. – СПб: СПб-региональное отделение РАЕН, 2011. − 416 с., илл.
2. АРБИТР, Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА) базовая версия 1.0 / Автор Можаев А.С. Правообладатель ОАО «СПИК СЗМА». // Свидетельство об официальной регистрации №2003611101. − М.: РОСПАТЕНТ РФ, 2003.

УДК 519.876.3

КОНЦЕПЦИЯ ПОСТРОЕНИЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ МАКРОУРОВНЕВОГО ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ВЫПОЛНЕНИЕМ ЗАДАЧ С ПРИМЕНЕНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ

Поленин Владимир Иванович[1], Можаев Александр Сергеевич[2], Можаева Ирина Александровна[2],
[1]Военный учебно-научный центр «Военно-морская академия»,
Россия, Санкт-Петербург, Ушаковская наб, 17/1,
[2]ОАО «Специализированная инжиниринговая компания «Севзапмонтажавтоматика»,
Россия, Санкт-–Петербург, В.О., 26-я линия, 15, корп.2, БЦ Биржа, эт. 10,
e-mails: polenin@mail.ru, asmozhaev@gmail.com

Аннотация: Рассматривается актуальная задача построения системы макроуровневого организационного управления выполнением целевых задач, функции которого на кораблях и судах традиционно принадлежат командному составу. Исторически управленческая деятельность на макроуровне целенаправленно не подвергалась автоматизированной поддержке ни в одной из известных систем управления. Для осуществления целевого управления на макроуровне должна подвергаться анализу вся располагаемая масса сведений о текущем состоянии объекта, процесса и возможных вариантах выполнения целевой задачи. Это качество становится доступным только при организации процесса управления на основе сетевых технологий и характеризует так называемые интегрированные системы управления. Обсуждаются технологические аспекты разработки системы или задачи автоматизированной поддержки макроуровневого организационного управления выполнением задач управления кораблем, судном, боевого управления, управления техническими средствами, борьбой за живучесть на основе сетевой информационной технологии.

Ключевые слова: *организационное управление; сетевые технологии; интегрированные системы управления; альтернативные сетевые планы; общий логико-вероятностный и детерминированный метод.*

THE CONCEPT OF CONSTRUCTING A SYSTEM OF AUTOMATED SUPPORT MACRO-LEVEL ORGANIZATIONAL MANAGEMENT TASKS WITH APPLICATION OF NETWORK TECHNOLOGIES

Vladimir Polenin[1], Alexander Mozhaev[2], Irina Mozhaeva[2],
[1]Voennyi educational-scientific center «Military-marine Academy»,
Russia, St. Petersburg, Ushakov nab., 17/1,
[2]JSC «Specialised engineering company «Sevzapmontazhautomatika»,

Russia, St. Petersburg, V. O., 26 line, 15, korp.2, BC Exchange, et. 10,
e-mails: polenin@mail.ru, asmozhaev@gmail.com

Abstract: Considers the actual task of constructing a system of macro-level organizational management targets, which on ships and vessels have traditionally belonged to the command staff. Historically, management activities at the macro level deliberately not been automated support in any of the known systems of control. To implement target management at the macro level should be analyzed all have a lot of information about the current state of the object, process and possible options for achieving target. This quality becomes available only when the organization's process-based management of network technologies and characterizes the so-called integrated management system. Discusses the technological aspects of the system development tasks or automated support macro-level organizational management tasks of control of the ship, vessel, command and control, control of technical means, the struggle for survivability based on network information technology.

Keywords: *organizational management; network technology; integrated management systems; alternative network plans; General logical-probabilistic and deterministic method.*

Введение. Необходимость организации функционирования системы управления выполнением целевых задач на основе сетевого планирования определяется тем, что эти задачи по своему многообразию, множеству агентов и сложности структурных взаимосвязей между ними могут оказаться недоступными для обзора (мониторинга) лицом-руководителем процесса выполнения задач (ЛПР).

Предлагается в системах управления сложными объектами вместо понятия «элемент» использовать понятие «операция» – в общем случае элемент сложной системы, участвующий в процессе выполнения задач целевой деятельности.

Все операционные модели объединяет важное существенное свойство: они активны в действиях или в состояниях. Глобальное поведение системы возникает как результат действий или 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.

Управляемое осуществление операций можно отождествить с наступлением соответствующих событий. События – второй общепринятый термин для широкого класса логических и вероятностных моделей.

В виде совокупности цепочек «операция-событие» можно представить систему или задачу управления нового типа − систему или задачу организационного управления другими системами организационно-технического управления, иначе говоря, систему управления выполнением целевых задач. Функции этой системы на кораблях и судах традиционно принадлежат командному составу. Автоматизация коснулась всех технических систем и процессов, но никогда не являлась целью предметной области макроуровневого управления кораблями и судами как управления выполнением целевых задач.

Управление выполнением задач – третий ключевой термин для предметной области управления кораблями и судами.

Почему важен переход от понятия «элемент» к понятию «операция»: с понятием «элемент» обычно возникает техногенный образ и техногенное, механистическое действие, связанные с размерностями и присущие системам управления техническими объектами и процессами. Для кораблей и судов это – управление движением (курсом, скоростью, глубиной), для технических средств – управление применением (включение, переключение, пуск, регулирование), для корабельных и судовых электроэнергетических систем – управление функционированием, для радиоэлектронных систем – управление наблюдением, для ракетно-артиллерийских систем – управление огнем, и т.п. И внутрисистемные связи для них насыщены потоками содержательной информации. Иначе говоря, понятие «элемент» обычно влечет за собой специфический техногенный образ из размерного предметного мира, и для его моделирования требуются специальные теории и информационные технологии.

Понятие «операция» может быть совершенно лишено предметного смысла. В результате выполнения или невыполнения операции наступает событие. Структурная взаимосвязь операций, отражаемая ориентированным графом со связями, характеризуемыми только и только булевыми логическими функциями «И», «ИЛИ», «НЕ», выходом которого является итоговое событие, означающее выполнение задачи и достижение цели действий, и представляет собой систему организационного управления выполнением задач.

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 объеме и 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.

Итак, множество операций и сложность структурных взаимосвязей между ними могут являться причиной затруднения или недоступности их обзора ЛПР. Кроме того, сложность осмысленного восприятия значительно возрастает в процессе выполнения задачи, развернутом во времени. Это обусловливается изменением внешней обстановки и состояния управляемой системы. Командно-сигнальное приведение в готовность, задействование или прекращение отдельных операций в управляемой системе могут выполняться не мгновенно, а с задержкой и, кроме того, завершаться отказами в выполнении операций.

Отслеживание этого процесса с помощью табло, мнемосхем и сигнальных датчиков современных автоматизированных систем управления кораблей и судов весьма непросто. Управляемая система образно представляет собой калейдоскоп взаимосвязанных операций, находящихся в различных состояниях. Неготовность или отказ некоторой операции или некоторой группы операций могут приводить либо к срыву выполнения задачи, либо к доступности лишь частичного ее выполнения. Широко известно, что трудности в оценке текущей обстановки, возможных путей и препятствий текущего развития процесса выполнения задачи, своевременного и осмысленного определения необходимой реакции ЛПР, являются характеристиками управленческой деятельности на макроуровне как одной из самых труднодоступных и требующих полной самоотдачи в процессе ее осуществления. Исторически управленческая деятельность на макроуровне целенаправленно не подвергалась автоматизированной поддержке ни в одной из известных систем управления.

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)».

Ниже рассматриваются основные аспекты разработки этой подсистемы или задачи на основе сетевой информационной технологии.

Информационно-технологические основы реализации. Концептуальное, формализованное описание постановки задачи, отражающее идеологию ее формирования, может быть представлено как устранение (минимизация) рассогласования (невязки) ΔS между вектором S текущего и вектором Z желаемого (целевого) состояния системы, осуществляемое управленческим действием U, опирающимся на доступные (допустимые, располагаемые) ресурсы $R_{доп}$ и время $T_{доп}$ в текущих условиях.

Для осуществления управления по достижению целевого состояния должна подвергаться анализу вся располагаемая масса сведений о текущем состоянии объекта и процесса управления, истории и возможных вариантах выполнения целевой задачи.

Это качество становится доступным только при организации процесса управления на основе сетевых технологий и характеризует так называемые интегрированные системы управления [2]. Сегодня такая информационная технология создана и она имеет название Сетевого общего логико-вероятностного и логико-детерминированного метода [1], [3].

Сетевой метод формализованного представления процесса макроуровневого организационного управления сводится к построению сетевого плана (СП) выполнения целевой задачи. Основой сетевого планирования является информационная динамическая сетевая модель, в которой весь комплекс задач и действий по выполнению целевой задачи расчленяется на отдельные, четко определенные операции (работы), располагаемые в строгой технологической последовательности их выполнения.

При анализе сетевой модели производится количественная, временная и стоимостная (затратная) оценка выполняемых операций (работ). Параметры задаются экспертами-специалистами для каждой входящей в сеть операции (работы) на основе здравого смысла, нормативных данных и практического опыта.

Технология создания сетевых планов выполнения целевых задач включает построение схемы функциональной целостности (СФЦ) сетевого плана и ее ввод в ПК АСМ АРБИТР [4], который в соответствии с заданными целями (критериями), ограничениями и допущениями автоматически строит все возможные варианты сетевых планов выполнения необходимых операций (работ) для достижения целевого события. Предполагается внедрение ПК АСМ АРБИТР в систему автоматизированного управления объектом и его сопряжение с системой датчиков состояния и внешних условий.

Схема организационного управления выполнением задач применительно к предметной области управления безопасностью морских судов [5] представлена на рисунке 1.

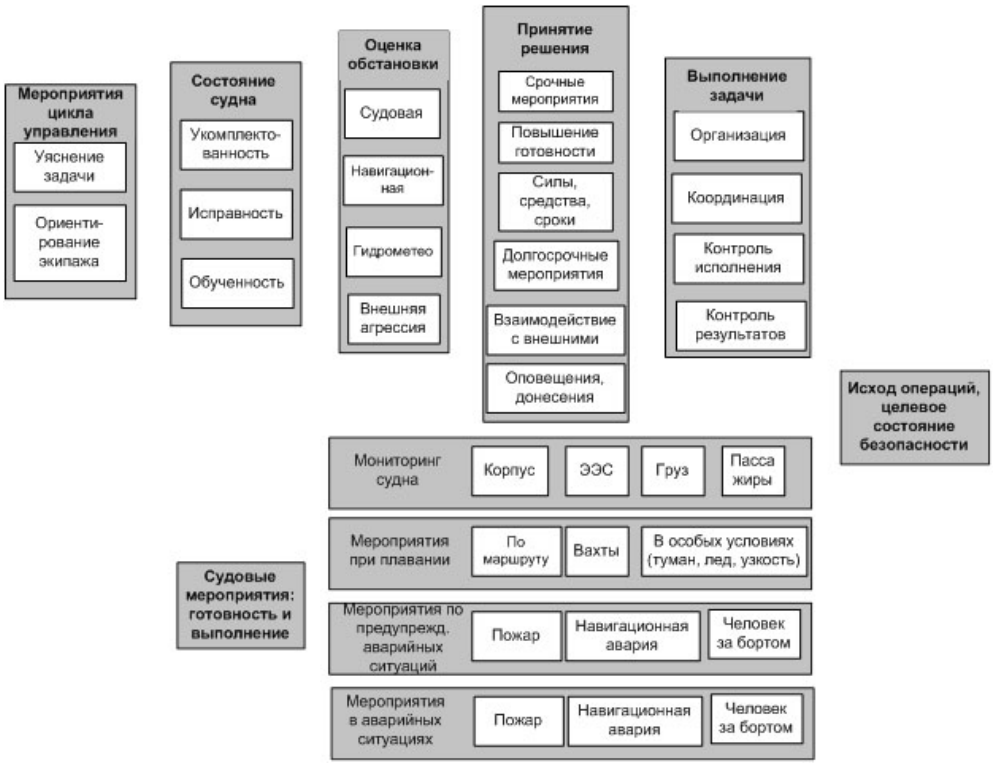


Рис. 1. Схема организационного управления безопасностью морских судов

Схема функциональной целостности (СФЦ) [1], [3], [4] сетевого плана системы автоматизированной поддержки макроуровневого организационного управления безопасностью морских судов представлена на рисунке 2.

Все операции этого сетевого плана являются обязательными, поэтому сетевой план содержит только конъюнктивные связи (тип PERT). Здесь для обеспечения компактности и обозримости сетевого плана используются так называемые ассоциированные вершины [4], имеющие внутренние операции, обозначенные фоновым рисунком. Невыполнение любой из операций связано с риском не достижения целевого состояния безопасности.

Наряду с безальтернативными сетевыми планами могут применяться альтернативные сетевые планы типа GERT. Пример такого предельно простого для обеспечения наглядности сетевого плана применительно к эпизоду самообороны корабля (судна) приведен на рисунке 3.

В зависимости от решения ЛПР и иных обстоятельств возможно применение либо только огневых средств самообороны, либо только средств РЭБ, либо огневых средств совместно со средствами РЭБ. Эти варианты характеризуются эффективностью самообороны, как показано на схеме.

С началом выполнения задачи включается сетевой план, состояния элементов корректируются в реальном масштабе времени по мере изменения ситуации и обстановки и отображаются на мнемосхеме СП, например, на АРМ ЛПР (вариант):

1. Серым цветом, если мероприятия не выполнены;
2. Белым цветом – по мере выполнения мероприятий;
3. Красным цветом – при техническом или функциональном отказе (невозможности выполнения);
4. Черным цветом, если выполнение мероприятий блокируется другими, предшествующими мероприятиями, например, при их отказах.

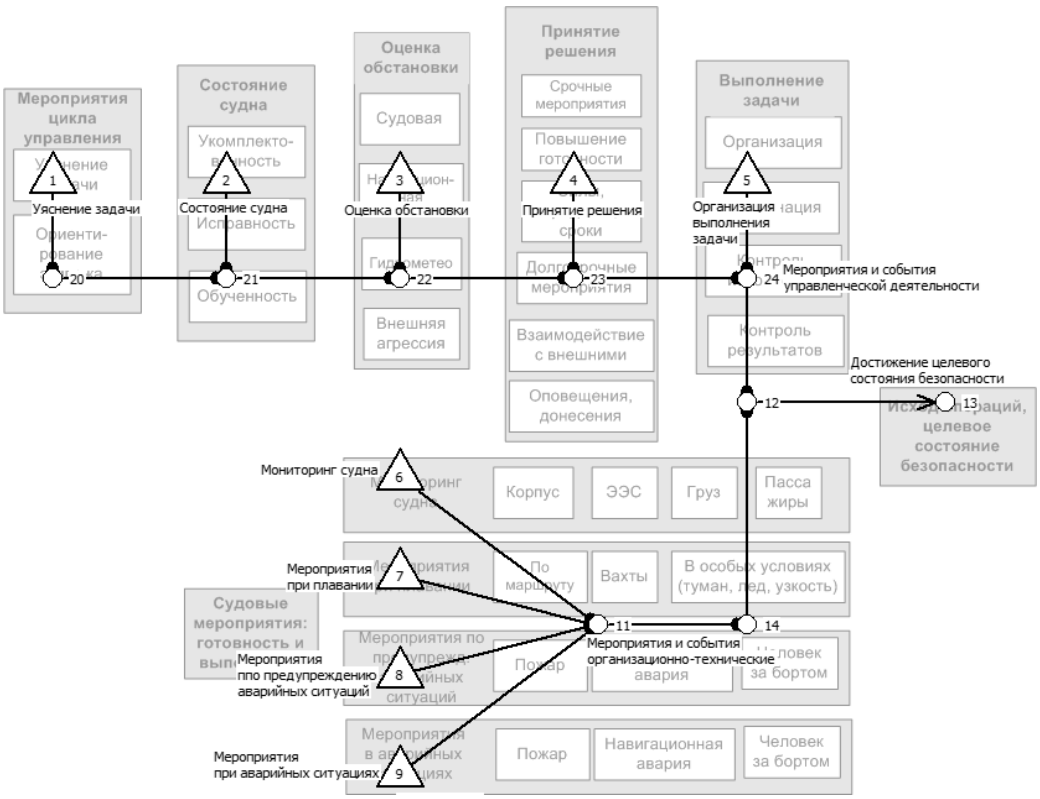


Рис. 2. СФЦ сетевого плана организационного управления безопасностью морских судов

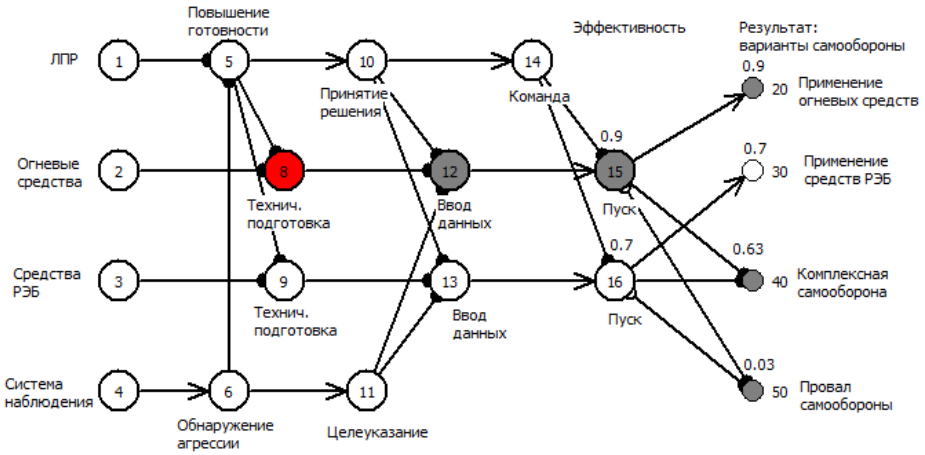


Рис. 3. СФЦ сетевого плана организационного управления эпизодом самообороны при техническом отказе огневых средств

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 такого рода поддержка управленческой деятельности командного и руководящего состава с использованием сетевых планов, реализуемых ПК АСМ АРБИТР, является целесообразной.

СПИСОК ЛИТЕРАТУРЫ

1. Можаев А.С., Поленин В.И. Сетевое планирование и управление – перспективный путь создания интегрированных систем боевого управления / Сборник трудов 12-й Международной научной школы «Моделирование и анализ безопасности и риска в сложных системах». – СПб: 2014. – С. 3-6.
2. Поленин В.И., Киваев Н.М., Сухачев Ю.А. Создание интегрированных систем боевого управления – высшая стадия комплексирования. – СПб: «Морская радиоэлектроника», № 2 (48), 2014. – С. 44-49.
3. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / В.И. Поленин, И.А. Рябинин, С.К. Свирин, И.А. Гладкова. Под ред. А.С. Можаева. – СПб: СПб-региональное отделение РАЕН, 2011. − 416 с.
4. Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА) АРБИТР, базовая версия 1.0 / Автор Можаев А.С. Правообладатель ОАО «СПИК СЗМА». // Свидетельство об официальной регистрации № 2003611101. − М.: РОСПАТЕНТ РФ, 2003.
5. Шарлай Г.Н. Управление морским судном. – Владивосток, Морской гос. ун-т, 2001. – 543 с.

УДК 621.396.6:681.3.06(075)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ХАРАКТЕРИСТИК СУШКИ СУДОВЫХ АСИНХРОННЫХ ДВИГАТЕЛЕЙ

Приходько Валентин Макарович, Приходько Ирина Валентиновна
ФГБОУ ВО «Государственный университет морского и речного флота
имени адмирала С.О. Макарова»
Россия, Санкт-Петербург, Комендантский проспект, д. 40, корпус 2, кв. 160
e-mail: prihodki-3@yandex.ru

Аннотация: Разработано математическое обеспечение для определения оптимальных параметров восстановления изоляции и представлены результаты математического моделирования характеристик сушки судовых асинхронных двигателей по энергосберегающей технологии на водном транспорте.

Ключевые слова: *математическая модель; характеристики сушки; асинхронные двигатели; энергосберегающие технологии.*

MATHEMATICAL MODELING OF DRYING CHARACTERISTICS OF SHIP ASYNCHRONOUS MOTORS

Prikhodko Valentin M., Prikhodko Irina V.
Admiral Makarov State University of Maritime and Inland Shipping (SUMIS)
Russia, 197373, Sankt-Peterburg, Komendantskiy Prospekt, 40, building 2, apt 160
e-mail: prihodki-3@yandex.ru

Abstract: Developed software to determine the optimal recovery options insulation and presents the results of mathematical modeling of drying characteristics of ship asynchronous motors with energy-efficient technologies for water transport.

Keywords: *mathematical model; characteristics of drying; induction motors; energy-saving technologies.*

Основой научно-технического прогресса является широкое использование электронно-вычислительной аппаратуры во всех областях техники, включая электрооборудование судов, электротехнические комплексы и судовые электроэнергетические системы. На современных автоматизированных судах различного назначения судовая электронно-вычислительная аппаратура представляет сложный комплекс устройств вычислительной техники, предназначенный для электронной обработки судовой информации, заключающейся в хранении, преобразовании и отображении ее в форму, удобную для восприятия экипажами судов. В настоящее время во всем мире наблюдается резкое увеличение такой аппаратуры морского исполнения, ее «интеллектуальности», быстродействия, объемов хранимой информации. На водном транспорте использование и внедрение электронно-вычислительной аппаратуры морского исполнения является одним из показателей обеспечения безопасности судоходства, мореплавания, повышения эффективности функционирования судовых электроэнергетических систем, электротехнических комплексов, единых высоковольтных электроэнергетических систем, микропроцессорных систем управления, систем управления, коммутации, защиты и диагностики. Прогресс в области судового электрооборудования, электронно-вычислительной аппаратуры морского исполнения, систем управления и статических полупроводниковых преобразователей электроэнергии (выпрямителей, инверторов, преобразователей частоты, преобразователей постоянного напряжения) определяется повышением надежности, экономичности, качества и эффективности устройств, совершенствованием конструкций и технологий. Препятствием повышения качества судовой электронно-вычислительной аппаратуры и сокращения сроков ее создания является несоответствие между возрастающей сложностью микроминиатюризации устаревшими методами и средствами ее конструирования. Разрешить это несоответствие способна инновационная технология проектирования, связанная с использованием и внедрением систем автоматизированного проектирования. Проблемы создания эффективных систем автоматизированного проектирования являются основополагающими.

Ускорение научно-технического прогресса и развитие науки - это неумолимое веление времени. Перевод экономики на рельсы интенсификации, рыночный путь развития эффективно возможен только на основе широкой компьютеризации всех отраслей промышленности и отрасли водного транспорта. Полная компьютеризация непосредственно связана с развитием и совершенствованием новой отрасли знаний – информационной технологии.

Считается, что на смену алгоритмам обработки данных в информационной индустрии приходит альтернативная информационная технология, т.е. технология автоформализации профессиональных знаний. Персональное ЭВМ (ПЭВМ) - это первый индивидуальный массовый инструмент активной формализации профессиональных знаний. Такие ЭВМ с «дружественным» по отношению к

пользователю программным обеспечением позволяют увеличить эффективность интеллектуальной деятельности человека. [1]

Выполнение такой программы невозможно без комплексной гибкой автоматизации проектирования и производства. Гибкая автоматизация - это новая глобальная концепция современного производства, базирующаяся на супер-, мини-ЭВМ, ПЭВМ, роботах и системах автоматизированного проектирования (САПР). Гибкие производственные системы (ГПС) – это высшая форма комплексной автоматизации производства, ориентированная на «безлюдную» технологию. Создание комплексов САПР-ГАП предусматривает разработку общей архитектуры автоматизированных производственных систем и общего математического обеспечения, связанных с интеграцией процессов проектирования и повышением качества производимого судового электрооборудования, электронной аппаратуры и систем управления морского исполнения. Комплекс средств автоматизации проектирования состоит из совокупности средств математического, лингвистического, программного, информационного, технического, методического и организационного обеспечений. Допускается рассматривать методическое обеспечение более широко, включая в него математическое и лингвистическое обеспечения.

САПР должна осуществлять автоматизированное проектирование на всех стадиях создания судового электрооборудования, электронно-вычислительной аппаратуры морского исполнения, судовых электротехнических комплексов, статических полупроводниковых преобразователей электроэнергии, микропроцессорных систем управления, коммутационно-защитных аппаратов, систем диагностики и судовых единых высоковольтных электроэнергетических систем судов с электродвижением. САПР должна внедряться на основе применения математических моделей, проектных процедур и средств вычислительной и организационной техники.

На основании «Стратегии развития судостроительной промышленности на период до 2020 года и на дальнейшую перспективу» одним из приоритетных направлений развития конкурентоспособной высокоэкономичной морской техники является, в частности, создание новых типов полупроводниковых преобразователей электрической энергии и разработка мобильных установок для контрольного прогрева, подсушки, сушки, восстановления сопротивления изоляции и диагностики изоляционных систем электрооборудования судов, обладающих повышенной надёжностью, безопасностью и живучестью. Важнейшим инструментом стратегии стала федеральная целевая программа «Развитие гражданской морской техники на 2009 – 2016 годы».

Разработаны портативные универсальные тиристорные преобразователи с перестраиваемыми структурами силовых вентильных модулей для обеспечения ресурсосбережения, снижения затрат энергии, повышения эффективности, интенсификации и оптимизации технологических режимов процесса контрольного прогрева, подсушки, сушки, восстановления сопротивления изоляции увлажнённых обмоток судового электрооборудования после зимнего отстоя речных судов, при судоремонте, а также в эксплуатационных условиях на водном транспорте [2], [3], [4]. Для судостроения и судоремонта рекомендован инновационный способ безразборной сушки увлажнённых обмоток судовых асинхронных двигателей (АД) электрическим током, управляемым энергосберегающими универсальными портативными тиристорными преобразователями с перестраиваемыми структурами силовых вентильных модулей [5], [6].

На основании проведённых исследований предложен новый способ пропитки обмоток судовых АД при одновременном нагреве пропитанных обмоток электрическим током, управляемым универсальными тиристорными преобразователями, и разработана инновационная технология пропитки – сушки статорных обмоток ремонтируемых АД в электроцехах судостроительно – судоремонтных предприятий [7].

В электроцехах судостроительно – судоремонтных предприятий и на судах речного, морского, рыбопромыслового флотов в судовых эксплуатационных условиях качество перемотки статорных обмоток в технологическом процессе ремонта асинхронных двигателей можно оценить при нагреве неподвижных электродвигателей, когда в обмотки статоров подаётся постоянный ток, управляемый с помощью портативных универсальных тиристорных преобразователей [8], [9], [10]. В этом случае можно просто, доступно, экономно, без дополнительных трудозатрат осуществить технологический процесс нагрева статорных обмоток АД и легко измерить температуру их в зависимости от времени. Идентичность этого процесса нагрева по всем трем обмоткам статора, а также характер этого процесса позволит оценить качество пропитки статорных обмоток, качество межсекционных соединений, равенство витков обмоток каждой из фаз. Переходный тепловой режим АД можно описать системой дифференциальных уравнений, которые учитывают тепловые связи между частями АД, теплоемкости этих тел и потери в них, в том числе в режимах прогрева, подсушки и сушки [11].

Для судовых АД эта система дифференциальных уравнений соответствует тепловой схеме замещения (рисунок 1) и имеет вид:

$$\left.\begin{aligned}
&\frac{d\theta_1}{dt}C_1+(\theta_1-\theta_2)a_{12}+(\theta_1-\theta_3)a_{13}+(\theta_1-\theta_6)a_{16}=P_1;\\
&\frac{d\theta_2}{dt}C_2+(\theta_2-\theta_1)a_{12}+(\theta_2-\theta_5)a_{25}=P_2;\\
&\frac{d\theta_3}{dt}C_3+(\theta_3-\theta_1)a_{13}+(\theta_3-\theta_4)a_{34}=P_3;\\
&\frac{d\theta_4}{dt}C_4+(\theta_4-\theta_3)a_{34}+(\theta_4-\theta_5)a_{45}=P_4;\\
&\frac{d\theta_5}{dt}C_5+(\theta_5-\theta_2)a_{25}+(\theta_5-\theta_4)a_{45}+(\theta_5-\theta_6)a_{56}=0;\\
&\frac{d\theta_6}{dt}C_6+(\theta_6-\theta_5)a_{56}+\theta_6 a_{60}=0
\end{aligned}\right\} \qquad (1)$$

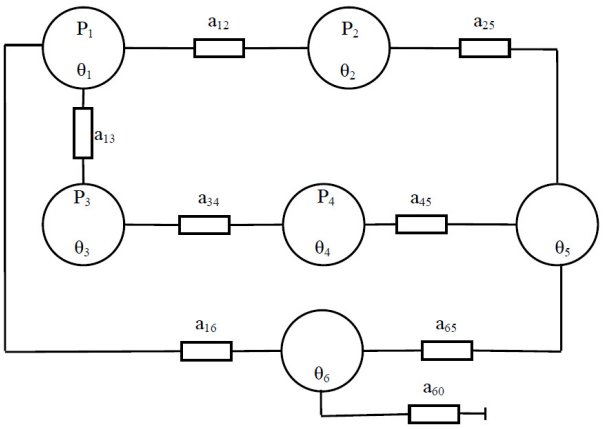


Рис. 1. Тепловая схема замещения судового асинхронного двигателя

В системе дифференциальных уравнений и на тепловой схеме замещения судового асинхронного двигателя: C_n – теплоемкости тел, Вт·с/град; a_{nk} – теплопроводности между телами, Вт/град; θ_n – превышение температуры тел, ºК; P_n – мощность потерь в телах, Вт; 1 – магнитопровод статора; 2 – магнитопровод и обмотка статора; 3 – пазная часть обмотки статора; 4 – лобовая часть обмотки статора; 5 – внутренняя полость воздуха АД; 6 – корпус судового АД.

Решение системы дифференциальных уравнений с расчетом теплопроводностей, теплоемкостей и потерь в частях АД производится на ПЭВМ численным методом Эйлера.

Конечно-разностная система уравнений при расчете теплового процесса имеет вид:

$$\left.\begin{aligned}
&\theta_{1n}=\theta_{1,n-1}+\frac{1}{C_1}(P_1-\theta_1 A_{11}-\theta_2 A_{12}-\theta_3 A_{13}-\theta_6 A_{16})\cdot h;\\
&.\\
&.\\
&\theta_{kn}=\theta_{k,n-1}+\frac{h}{C_k}(P_k-\sum_i \theta_{i,n-1}A_{ki}),
\end{aligned}\right\} \qquad (2)$$

где h – шаг вычислений, с; A_{ki} – элементы матрицы коэффициентов при θ.

Величина шага по времени зависит от постоянных времени процесса, и его значение должно быть меньше самой малой постоянной времени системы. Оптимальное значение шага определяется опытным путем с учетом целесообразного упрощения системы уравнений (1), а также корректировкой по экспериментальным данным.

Следует отметить, что при нагреве постоянным по величине током необходимо учитывать изменение сопротивлений статорных обмоток. Это уточнение выполняется с помощью уравнений для обмоток статора:

$$\left.\begin{aligned}
P_{3(k)}&=P_{3(0)}\left(1+\frac{\theta_{3k}}{235+t_{окр}}\right);\\
P_{4(k)}&=P_{4(0)}\left(1+\frac{\theta_{4k}}{235+t_{окр}}\right),
\end{aligned}\right\} \qquad (3)$$

где $t_{окр}$ – температура окружающей среды; θ_k – превышение температуры на к-ом шаге.

На рис. 2 и 3 даны экспериментальные и расчетные по (1) данные для АД типа 4АХ90L4У3 номинальной мощностью, равной 2,2 кВт. Экспериментальные и расчетные данные с достаточной точностью совпадают. Однако, необходима дальнейшая корректировка методики расчета с учетом экспериментальных данных, так как тепловые связи между статорной обмоткой и пакетом частей статора зависят от качества пропитки обмоток, которая может быть разной. Поэтому необходимо проводить дальнейшие исследования, чтобы уточнить достоверность характера процесса нагрева исправной обмотки. При рассмотрении только качественной стороны теплового процесса в АД целесообразно упростить систему уравнении (1) таким образом, чтобы получить ее аналитическое решение. Такое относительно простое решение получается, если рассматривать систему двух тел – обмотки статора и корпуса с магнитопроводом статора с учетом теплоотдачи от корпуса и лобовых частей обмотки статора в окружающую среду.

Система дифференциальных уравнений для этого случая имеет вид:

$$\left.\begin{aligned} &\frac{d\theta_1}{dt}C_1 + (\theta_1 - \theta_2)a_{12} + \theta_1 a_{10} = P_1; \\ &\frac{d\theta_2}{dt}C_2 + (\theta_2 - \theta_1)a_{12} + \theta_2 a_{20} = P_2, \end{aligned}\right\} \qquad (4)$$

где 1 – обмотка статора; 2 – магнитопровод и корпус статора; a_{10}, a_{20} – теплоотдача в окружающую среду от лобовых частей обмотки статора и корпуса, Вт/град.

Решение системы (4) следующее:

$$\theta_{1уус} = \frac{P_1(a_{20} + a_{12})}{a_{10}a_{20} + a_{10}a_{12} + a_{20}a_{12}}, \text{ К}$$

$$\theta_{2уус} = \frac{P_1}{a_{20}} - \theta_{1уус}\frac{a_{10}}{a_{20}}, \text{ К}$$

$$T_1 \approx \frac{C_1}{a_{10} + a_{12}}, \text{ с}$$

$$T_2 \approx \frac{C_1(a_{10} + a_{12})}{a_{10}a_{20} + a_{10}a_{12} + a_{20}a_{12}}, \text{ с}$$

$$\theta_{11} = \frac{\frac{P_1}{C_1}T_1T_2 - \theta_{2уус}T_2}{T_1 - T_2}, \text{ К} \qquad (5)$$

$$\theta_{21} = \frac{\frac{P_2}{C_1}T_1T_2 - \theta_{2уус}T_2}{T_1 - T_2}, \text{ К}$$

$$\theta_{12} = \theta_{1уус} - \theta_{11}, \text{ К}$$

$$\theta_{22} = \theta_{2уус} - \theta_{21}, \text{ К}$$

$$\theta_1 = \theta_{11}(1 - e^{-t/T_2}) + \theta_{12}(1 - e^{-t/T_1}), \text{ К}$$

$$\theta_2 = \theta_{21}(1 - e^{-t/T_2}) + \theta_{22}(1 - e^{-t/T_1}), \text{ К},$$

где T_1,T_2 – постоянные времени процесса, с;$\theta_{1уст}$, $\theta_{2уст}$ – установившиеся превышения температуры, К.

На рис. 2 и 3 показаны кривые нагрева обмоток статора судового асинхронного двигателя постоянным током, регулируемым тиристорным преобразователем, в сравнении с опытными и расчетными данными по (1) и (5), где видно, что точность расчетов по (5) для больших токов ниже. Однако выражение (5) после соответствующей корректировки по опытным данным может служить основой для управления процессом нагрева АД в режиме прогрева, подсушки, сушки с помощью микропроцессора с учетом допустимой погрешности.

Для обеспечения ресурсосбережения, снижения энергетических затрат, повышения эффективности, интенсификации и оптимизации технологических режимов процесса прогрева, подсушки, сушки, восстановления сопротивления изоляции увлажненных обмоток судовых асинхронных двигателей после зимнего отстоя речных судов, при судоремонте, а также в эксплуатационных условиях на водном транспорте проведены исследования процессов внутреннего

тепломассопереноса в увлажненной изоляционной системе при управляемом токовом нагреве статорных обмоток электродвигателей судового исполнения.

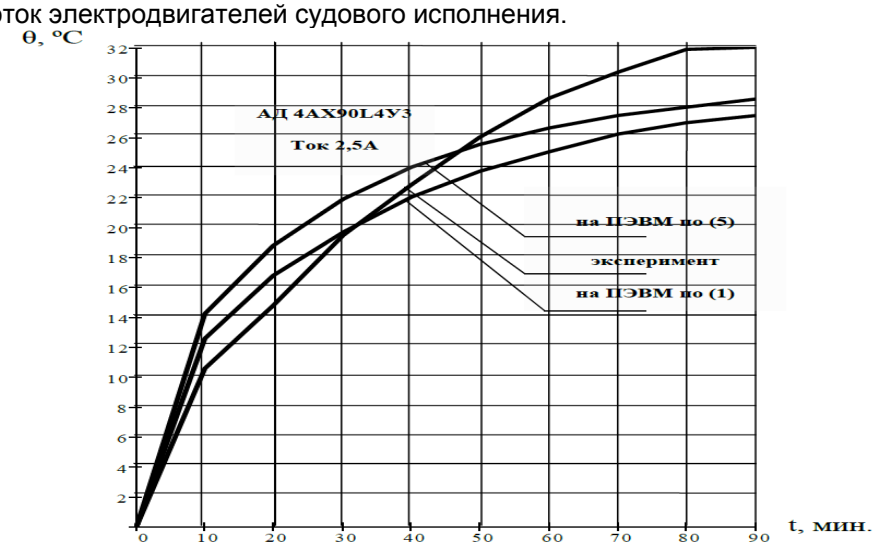


Рис. 2. Нагрев обмоток судового асинхронного двигателя постоянным током, регулируемым тиристорным преобразователем

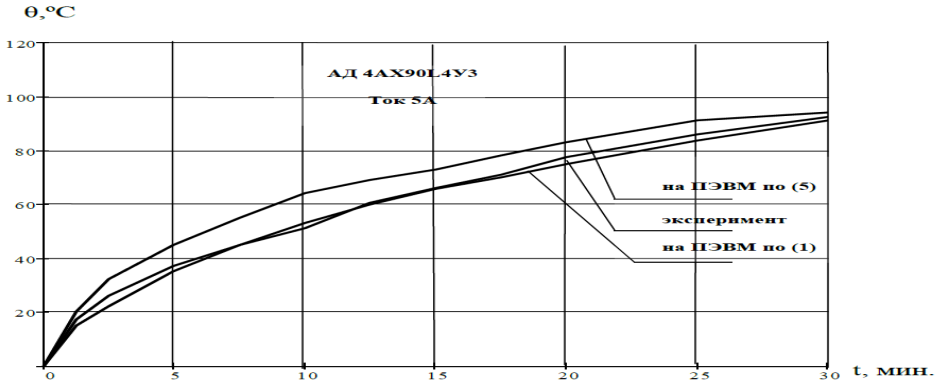


Рис. 3. Нагрев обмоток судового асинхронного двигателя постоянным током, регулируемым тиристорным преобразователем

Теоретически обоснован и разработан инновационный энергосберегающий рациональный способ повышения эффективности и увеличения интенсивности токовой сушки изоляции отсыревших обмоток асинхронных двигателей при судоремонте на судостроительно-судоремонтных предприятиях.

СПИСОК ЛИТЕРАТУРЫ

1. Громов Г.Р. Национальные информационные ресурсы: проблемы промышленной эксплуатации / Г.Р. Громов. - М.: Наука, 1984. - 240 с.
2. Приходько В.М. Портативный тиристорный преобразователь с перестраиваемой структурой/ В.М. Приходько// Труды II Международного научно – технического семинара «Исследование, проектирование и эксплуатация судовых ДВС», 27 сентября 2007 г. – СПб.: СПГУВК, 2008. – С. 282-298.
3. Приходько В.М. Энергосберегающий универсальный тиристорный преобразователь/ В.М. Приходько// Судостроение. – 2000. - №1. – С. 44-45.
4. Приходько В.М. Компактный универсальный тиристорный преобразователь с перестраиваемой структурой/ В.М. Приходько, А.А. Адам, Е.Б. Логинов, Э.М. Огородов, А.М. Приходько// Наука и техника на речном транспорте. – 2001. - №7. – С. 17-24.
5. Приходько В.М. Методы и технические средства комплексных испытаний элементов судовых электроэнергетических систем в судостроении и судоремонте: научная монография/ В.М. Приходько. – СПб.: ИПЦ СПГУВК, 2005. – 348 с.
6. Приходько В.М. Интенсификация комплексных испытаний судового электрооборудования по энергосберегающей технологии в судостроении и судоремонте: научная монография/ В.М. Приходько. – СПб.: СПГУВК, 2013. – 244 с.
7. Приходько В.М. Новая технология пропитки и управляемой токовой сушки электродвигателей/ В.М. Приходько // Морской транспорт. Экспресс – информация. Серия. Техническая эксплуатация флота и судоремонт. – М.: ГУП Мортехинформреклама, 2002. – Вып. 8 (920). С. 1-11.
8. Приходько В.М. Переносный универсальный тиристорный преобразователь с перестраиваемой структурой/ В.М. Приходько, В.И. Кравченко, А.М. Приходько// Промышленная энергетика. – 1999. - №4. – С.30 – 35.
9. Приходько В.М. Тиристорный преобразователь – регулятор универсального назначения/ В.М. Приходько, В.И. Кравченко, А.М. Приходько// Промышленная энергетика. – 1994. - №5. – С.14-19.
10. Приходько А.М. Универсальный тиристорный преобразователь/ А.М. Приходько, В.М. Приходько, В.И. Кравченко// Механизация и электрификация сельского хозяйства. – 1999. - №4. – С. 13-15.
11. Гольберг О.Д. Проектирование электрических машин/ О.Д. Гольберг, Я.С. Гудин, И.С. Свириденко. – М.: Высшая школа, 1984. – 430 с.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 303.01

ГЛАВНАЯ ПРИЧИНА РАСПАДА СССР

Кефели Игорь Федорович, Меркулов Андрей Львович,
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова,
Россия, Санкт-Петербург, ул. Краснопутиловская, д. 20, кв. 65,
e-mails: geokefeli@mail.ru, merrkkjjander@mail.ru

Аннотация: Это статья посвящена выяснению основных причин распада СССР.

Ключевые слова: *СССР; Римская империя; эволюция; уровень развития.*

THE MAJOR REASON OF THE COLLAPSE OF THE USSR

Igor' Kefeli, Andrei Merkulov,
The Baltic State Technical University, named after D.F. Ustinov,
Russia, St. Petersburg, Krasnoputilovskay Street 20, flat 65,
e-mails: geokefeli@mail.ru, merrkkjjander@mail.ru

Abstract: The article delicates to causing the main solutions of the collapse of the USSR.

Keywords: *USSR; Roman Empire; evolution, level of development.*

Все мы видим стремительное внедрение технологий во все сферы нашей жизни – экономическую, политическую, социальную, культурную, военную. Это понятие – информационная безопасность родилось с появлением компьютера, интернета, мобильной связи. 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.

Что такое информационная война? Это управление информационными потоками в определенных целях, управление и явное, и тайное для достижения необходимых результатов. Распад СССР по мнению многих специалистов – результат успешной, долговременной информационной войны, общий замысел которой был изложен в конце Второй Мировой войны. Известно, как это было. В 1945 году создается штаб информационной войны против СССР во главе с Даллесом. Главное в стратегии такой войны – целенаправленное информационно-психологическое воздействие по всем возможным каналам на общественное мнение населения. С интересом слушали «Голос Америки» по вечерам по своим радиоприемникам наша молодежь. В 1957 году в Москве состоялся всемирный фестиваль молодежи и студентов, где наши молодые люди общались с иностранной молодежью и впервые узнавали о высоком материальном уровне жизни в западных странах. Диссиденты появились в СССР в 60^{е} годы, их деятельность расширялась, появилась и превращалась в активную антисоветская «пятая колонна». Публично началось обсуждение прав человека в СССР в информационном пространстве. 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.

Можно назвать и другую причину – слабость интеллектуального и стратегического мышления руководителей советского государства в последние двадцать-тридцать лет его существования, их неспособность своевременно осознать необходимость перемен во внутренней и внешней политике и экономике государства. Кадры, которые тогда руководили идеологией в СССР, не смогли увидеть внешние информационные угрозы и соответственно на них отреагировать.

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 доказанными, научно-необоснованными, но, однако, я все же попытаюсь на своем уровне выразить отношение к этой важной теме.

Вся история человечества состоит из череды кардинальных реконструкций. Издавна люди стремились понять и объяснить ход истории. История – не только память человечества, но и средство познания закономерностей исторического процесса развития, его логика. Уяснить эту логику можно на примерах многих цивилизаций. Однако, история народов, дальше других продвинувшихся по пути исторического прогресса, позволяет с большим основанием судить о законах и перспективах развития обществ. Известные экономисты, политологи, государственные деятели, разделяя мнение о катастрофическом состоянии России, предлагают различные меры по исправлению ситуации, но к единому мнению не приходят. Основанием их выводов является анализ развития народов и государств в основном за последнее столетие, можно сказать нашей современности. Но ведь современность вырастает из предыдущих веков, где имели место схожие события и было бы интересно и полезно посмотреть, как они протекали, хотя они и происходили на другом уровне. Мало говорится о роли эволюционных процессов в развитии государств и народов или уже считается, что человечество достигло таких высот в развитии, что можно ими пренебрегать? Эволюция – широкое, многообразное понятие, но в нашем случае необходимо хотя бы приблизительно уяснить триединое направление тесно связанных процессов – эволюции природы, эволюции человека и эволюции человеческих обществ. Если об эволюционных процессах в природе нам многое известно на основании теорий о естественном развитии органического мира, созданных и убедительно научно разработанных французским ученым Ж. Ламарком и английским ученым Ч. Дарвином, то об эволюции человеческих обществ, их формах, их развитии наши знания недостаточны, хотя имеются несколько теорий по этому вопросу, но нет единой, общепризнанной. Можно выразить графически в общей форме процессы эволюции общественных формаций, человека и природы по времени. Они имеют разные законы развития, но они имеют во многом и параллельные черты, по форме разные, но схожие по содержанию. Это понятно, поскольку сам человек является производным органического мира. На графике эволюций мы видим три расходящиеся экспоненты. Видим все шире расходящиеся во времени процессы развития самого человека и природы, уровень которой направлен к снижению и так же расходящиеся во времени процессы развития человека и общественных формаций. О первом разводе написано массы книг и исследований, горы диссертаций и научных объяснений. О втором – меньше. Всем известен биологический процесс развития; из самых приспособленных среди простейших организмов через непрерывную цепь поколений развилось все существующее многообразие видов. Отдельные онтогенезы в этой цепи складываются в единую последовательность – гологению, отдельные жизненные циклы – в историческую причинную цепь в так называемую «спираль гологенеза». Появляется возможность прогресса – эволюции в направлении оптимального функционирования в существующих условиях.

Для приближенного анализа событий и выяснения вопроса темы о главной причине гибели СССР я предположил, что наиболее полную картину эволюции общества в классическом выражении можно увидеть в полном цикле развития общества в завершающем периоде рабовладельческой формации. В этом случае мы ясно увидим все фазы развития государства, хотя оно и будет отличаться по уровню от других государств; а также длительность каждой фазы. Таким государством, причем наиболее развитым (а нам такое и нужно) представляется Римская империя. В дальнейшей истории – в феодальном, феодально-крепостническом, капиталистическом формах эта «классическая» эволюция обществ нарушается под влиянием развития человека и природы и принимает все более измененную конфигурацию по мере приближения к нашей современности.

Мне могут сразу возразить, – «позвольте, позвольте, это же не научный подход. Вы берете для анализа крупнейшую империю двухтысячелетней давности, когда были одни законы организации общественных формаций, в значительной степени подверженные эволюционным процессам и сильнейшее государство современности, когда действуют другие законы организации обществ, когда эволюционные процессы в значительной степени направляются самим человеком» Но 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. Академик В.И. Вернадский писал: «Геологический эволюционный процесс отвечает биологическому единству и равенству всех людей. Нельзя безнаказанно идти против принципа единства всех людей как закона природы. Человечество в целом не является самодостаточным живым существом, его существование обусловлено взаимосвязью и единством с природой» Но, как говорится, «Слава Богу», что до такого критического состояния мы еще не доехали и матушка-природа еще в состоянии путем жестких наказаний подправлять наши опасные «завихрения». Об этой взаимности я скажу два слова в заключении, тем более, что это связано с одной из тем нашей конференции – проблемы устойчивого развития. Вернемся к теме данной работы.

В истории народов мы видим удивительную эволюцию двух крупнейших империй мира – Римской империи в эпоху рабовладения и советской империи – СССР в период социализма. Римская империя существовала восемьсот лет до своего распада, СССР существовал 70 лет. Разница в длительности процессов развития весьма существенная даже при учете того, что скорость эволюционных процессов в эпоху рабовладения была несравнимо ниже современных. Росту производительных сил, культуры, искусства, мощи римской армии не было препятствий. Все противники Рима терпели поражения; периоды войн, передовой политический строй, экономическое благополучие, высокие нравственные идеалы поддерживали в правящем классе и гражданах республики достаточно высокий уровень пассионарности. Римская империя достигла невероятного для того времени уровня развития, и этим она значительно возвысилась над окружающими народами. Она вышла из неких пределов прогресса своего времени.

В случае Советского Союза ситуация сложилась другая. В мире родилась первая страна с социальным укладом, направленным на удовлетворение потребностей всего народа, а не какого-то одного класса. Частная собственность отменялась. Такого в мировой истории еще не было. Одним своим появлением Советского Россия создала напряженность в мировом сообществе. Ее окружали страны, для которых частная собственность – основа существования и молодая социалистическая страна сразу получила образ врага цивилизации.

Предлагаемая причина разрушения СССР выглядит неправдоподобно, почти фантастически, но мало ли в нашей жизни событий и явлений, каким-то невероятным образом попадающих в наше сознание и заставляющих нас думать.

Вначале я установил приблизительно длительность фаз развития Римской и Советской империй. Затем определил также приблизительно условные различия и сходство в государственной деятельности. За неимением времени не буду их перечислять. Они были сведены в таблицы, и 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.

Затем были составлены графики фаз развития по времени существования. Под уровнем развития мы обычно подразумеваем развитие экономики, политики, военного дела, социальной сферы. 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. (Понятно, что уровень развития СССР возможно в сотни раз превышал уровень Римской державы.) Какой-то могучий выплеск в эволюции – стремительно высокий взлет и столь же стремительное падение, как вспышка неведомой энергии. Как будто история нам говорит: «Вот, смотрите. Пример нового общества. В нем много преимуществ, но оно не без недостатков. Ваше дело, принимать это общество или отвергать его»

Мы знаем, что смена одного типа общества другим происходит в течение какого-то переходного периода. В случае с появлением СССР никакого перехода, как такового, к социализму не было. Было внезапное, неожиданное в мире, ослепительно-яркое явлением социализма, возможно показавшее человечеству его будущее.

Имеютя ли общие законы эволюции обществ, подобные законам эволюции в природе? Вот как объясняет эту тему наш выдающийся русский ученый-социолог А. А. Зиновьев: «Эволюция общества есть массовое явление. Всякое общество есть нечто изменчивое и в то же время устойчивое. В нем постоянно происходят какие-то отклонения от некой формы. Но есть и механизм, удерживающий его в пределах некой нормы. Происходит уничтожение индивидов, заметным образом отклоняющихся от нормы, а также распределение среди массы индивидов полезных или неопасных отклонений отдельных членов (например, новое знание, добытое одним, становится всеобщим достоянием). Появляются экземпляры, заметно отклоняющиеся от нормы. Если несмотря на борьбу с ними они появляются снова и снова, эти отклонения становятся привычными. К ним привыкают, их признают. Их усваивают другие. И происходит сдвиг всего объединения от бывшей нормы. Здесь диалектика

права: нужно количественное накопление для качественного «скачка». Но на такой процесс нужно время» [2].

На основании вышесказанного можно предложить следующий вывод. В период появления и существования Советского Союза мировая капиталистическая система была ещё сильна. Она еще не собиралась отживать, еще наращивала свою мощь и влияние на мировые события. То есть явление социализма было заметным отклонением от действовавшей в данное время некой нормы эволюции, пробным показом возможного будущего человечества, но в существующих условиях обреченного на гибель с тем, чтобы появиться снова в лучшем качестве на смену капитализму.

Иначе говоря, это явление новой, социалистической формации было явлением преждевременным!

Преждевременное появление на арене Истории – вот третья и самая главная причина гибели молодого Советского государства.

Вернемся теперь к вопросу о постоянном стремлении человека к познанию мира, к дальнейшему развитию, невольно при этом и неизбежно нарушая и попирая законы природы. Вот что пишет на эту тему А. Зиновьев: «Во второй половине XX века произошел перелом в самом типе эволюционного процесса: степень и масштабы сознательности исторических событий достигли такого уровня, что стихийный эволюционный процесс уступил место проектируемой и управляемой эволюции. Это, напоминаю, не означает, будто все в эволюции человечества стало планироваться и ход эволюции стал управляться в соответствии с планами. Это означает, что целенаправленный, планируемый и управляемый компонент эволюционного процесса стал играть определяющую роль в конкретной истории человечества» [1]. И в другом месте – «Средства массовой информации запугивают общество последствиями вторжения в биологический механизм наследственности людей и в механизм развития зародышевых клеток зрелых организмов. Но уже произошло нечто более страшное, а именно – люди вторглись в механизм социальной эволюции человечества. Разрушительные последствия этого вторжения дают знать о себе очевидным образом уже теперь, а о причинах их не говорится ни слова. Более того, выяснение этих причин и предание их широкой гласности является фактически запретным или настолько затрудненным, что те сведения, который как-то доходят до сознания масс, остаются без всяких последствий» [2].

Взаимоотношения человека и природы – одно из главных основ устойчивого развития общества, но есть и другая основа, не менее важная и более сложная – политическая. В группе государств примерно схожего социального строя намного больше возможностей устойчивого развития чем одной стране в окружении государств другой политической системы. Но даже и в такой группе, если в ней имеется государство несравнимо мощнее остальных, то часто у такого государства появляется стремление подчинить себе в той или иной мере другие государства в своих интересах. И тут тоже появляются трудности неравномерности развития. Умнейшие, справедливые, неустанные борцы за права человека (как они сами о себе говорят) американцы, придумали и организовали движение терроризма, объявили теперь какой-то «управляемый хаос», раздербанили Ближний Восток, хотя люди там жили вполне достойно, навели смуту в Северной Африке, создали там невыносимые условия жизни и направили потоки беженцев через море в Европу, убеждая при этом Европу, что во всем виновата Россия.

Что же может натворить на Земле человек на этом пути безудержного развития. Мы давно уже видим, что он может. Еще только открыв секрет атомной энергии, он изготовил атомную бомбу и бросил ее на города; не разобравшись еще в последствиях применения этой энергии, понастроил по миру атомных электростанций, которые отравили на многие десятилетия огромные пространства в разных странах. Клонировал овцу и обещал в скором времени клонировать людей по требуемым параметрам.

Так где же 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.

СПИСОК ЛИТЕРАТУРЫ

1. Зиновьев А.А, Запад: Избранные сочинения – М.: Апрель, 2008, 512с.
2. Зиновьев А.А. Логическая социология: Избранные сочинения – М.: Астрель, 2008, 606с.
3. Панарин И. Первая мировая информационная война. Развал СССР – СПб.: Питер, 2010, 256с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.8

ПРОТОТИП КОМПЛЕКСА ПРОГРАММ ДЛЯ АНАЛИЗА ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫЙ НА ОСНОВЕ АЛГОРИТМОВ ОБХОДА ГРАФОВ СОЦИАЛЬНЫХ СВЯЗЕЙ ПОЛЬЗОВАТЕЛЕЙ

Азаров Артур Александрович[1,2,3], Абрамов Максим Викторович[1,2,3], Тулупьев Александр Львович[1,3], Тулупьева Татьяна Валентиновна[1,3],
[1] Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14-я линия В.О., д. 39,
[2] Московский государственный гуманитарный университет им. М.А. Шолохова,
Россия, Москва, Верхняя Радищевская ул., д. 16-18,
[3] Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7-9,
e-mails: artur-azarov@yandex.ru, mva16@list.ru, alexander.tulupyev@gmail.com, tvt100a@mail.ru

Аннотация: В статье представлен прототип программного продукта, предназначенный для анализа защищенности пользователей информационных систем от социоинженерных атакующих воздействий злоумышленника. В программном продукте реализован ряд близких по принципу работы алгоритмов, но существенно различающихся в быстродействии.

Ключевые слова: *информационная безопасность; социоинженерные атаки; защита пользователя.*

PROTOTYPE OF SOFTWARE FOR ANALYSIS OF PROTECTED OF USERS OF INFORMATION SYSTEM CONSTRUCTED ON THE BASIS OF ALGORITHM GRAPH TRAVERSAL SOCIAL TIES USERS

Artur Azarov[1,2,3], Maksim Abramov[1,2,3], Alexandr Tulupyev[1,3], Tatyana Tulupyeva[1,3],
[1] St. Petersburg institute for informatics and automation of the Russian academy of sciences,
Russia, St. Petersburg, 14 Line, 39,
[2] Sholokhov Moscow State University for the humanities,
Russia, Moscow, Verhnyaya Radishchevskaya, 16-18,
[3] St.Petersburg State University,
Russia, St. Petersburg, Universitetskaya nab., 7-9,
e-mails: artur-azarov@yandex.ru, mva16@list.ru, alexander.tulupyev@gmail.com, tvt100a@mail.ru

Abstract: The paper presents a prototype of the software used to analyze the security of users of information systems from attacking the socio-engineering actions the attacker. In the software product implemented a number of relatives on the basis of algorithms, but significantly different in performance.

Keywords: *Information Security; social engineering attacks; user protection.*

Введение. Ведение успешного современного бизнеса требует активного привлечения компьютерных систем к хранению и обработке больших массивов информации. Такое широкое применение данного инструмента требует привлечения особого внимания к обеспечению безопасности хранимой и обрабатываемой информации. Как показывают исследования [3], атаки на информационные системы стали происходить чаще, кроме того, они приносят большие убытки и требуют больше ресурсов и времени для установления виновных в подобных преступлениях. Всемирное исследование 2014 года с участием компаний из США, охватившее семь стран, показало, что средний размер убытков американских компаний от киберпреступлений вырос более чем на 9%, до 12,7 миллиона долларов. В исследовании за 2013 год это значение составляло 11,6 миллиона долларов. Среднее время, необходимое для расследования атаки на информационную систему, также выросло. Теперь оно составляет 45 дней по сравнению с 32 днями в 2013 году [3]. Данная тенденция основана также на том, что атаки злоумышленников на информационные системы всё чаще имеют не только программно-технический характер, но и начинают затрагивать пользователей информационной системы, то есть, становятся социоинженерными. Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить её

безопасность (конфиденциальность, целостность или доступность) [1], [2].

Целью данной статьи является описание программного модуля, предназначенного для расчета вероятности резистентности пользователей информационных систем к социоинженерным атакующим воздействиям злоумышленника.

Алгоритмы подсчета вероятности резистентности пользователей к социоинженерным атакующим воздействиям злоумышленника. Подсчет вероятности резистентности определенных пользователей сети к социоинженерным атакующим воздействиям злоумышленника говорит о защищенности данного узла, то есть пользователя, а не о защищенности системы в целом. Для подсчета совокупной вероятности защищенности информационной системы от социоинженерных атак злоумышленника можно пользоваться несколькими эвристиками. Одним из возможных подходов является подход к подсчету данной вероятности с помощью поиска всевозможных путей в графе. Общая схема ключевых шагов подобного алгоритма выглядит следующим образом. Изначально у злоумышленника есть один кандидат для атаки. Для удобства, и, не умаляя общности, присвоим ему номер один. После этого предполагаем, что у любого из пользователей может оказаться доступ к требуемому злоумышленнику файлу, и ищем вероятности успешности социоинженерной атаки злоумышленника на каждого пользователя, учитывая при этом веса перехода от пользователя к пользователю.

На рис. 1 представлен пример межличностных связей персонала информационной системы. У каждого сотрудника указана вероятность успешности социоинженерного атакующего воздействия злоумышленника на него. В данном случае, под вероятностью успешности социоинженерного атакующего воздействия злоумышленника понимается совокупная вероятность успешности социоинженерной атаки на пользователя в случае применения всех выявленных социоинженерных атакующих воздействий. Между пользователями существуют связи, «взаимоотношения». Каждая подобная связь имеет собственный вес, то есть вероятность успешного перехода по этой связи в случае социоинженерного воздействия злоумышленника.

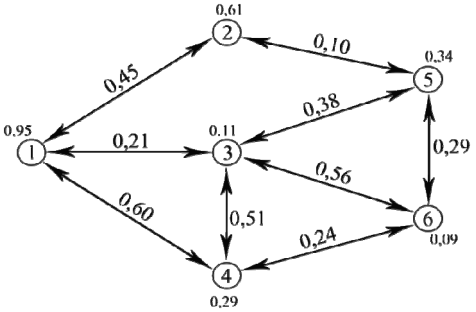


Рис. 2 Пример межличностных связей персонала информационной системы

Пусть P_i — вероятность успешности атаки на i-того сотрудника, если у злоумышленника есть на него выход, P_{ij} — вероятность выхода злоумышленника на пользователя j через пользователя i, если пользователь i уже успешно атакован. Тогда вероятность пути в графе отношений от пользователя m до пользователя j через пользователей i_k: $\tilde{P}_{m-\ldots-i_k-\ldots-j} = P_m \prod_{k=1}^{n-1} (P_{i_k, i_{k+1}} P_{i_{k+1}})$, где $i_1 = m$, $i_n = j$. Теперь, когда у нас есть вероятность атаки на данного пользователя j через цепь пользователей, вычислим формулу атаки через несколько цепей пользователей $\tilde{P}_i$: $\tilde{P}_{\mathrm{sum}j} = 1 - \sum_{i=1..k} (\tilde{P}_i)$. Соответственно чтобы $\tilde{P}_{\mathrm{sum}j}$ была полной вероятностью успешности атаки на пользователя j, нужно чтоб цепи были полным множеством всевозможных путей, либо аппроксимировали его.

Преимущества данного метода заключаются в том, что он рассчитывает точную вероятность и прост в понимании. В то же время, при больших объемах данных, возникает огромное количество цепей с небольшим весом (то есть с ничтожно малой вероятностью). Кроме того, для каждого из пользователей вероятность нужно пересчитывать отдельно.

Второй подход заключается в обходе в ширину, где у каждого сотрудника будем вычислять вероятность успешности проведения социоинженерной атаки через него на всех пользователей, с которыми у него есть ребро в графе межличностных связей пользователей системы. Причем учитывать будем только связи с пользователями, находящимися на одном уровне с рассматриваемым сотрудником, и пользователей, находящихся на уровнях ниже. Под фразой «находятся на одном уровне» будем подразумевать, что длина минимального пути в графе межличностных связей между первой жертвой злоумышленника и данными пользователями одинакова. «Уровень ниже», соответственно обозначает, что длина минимального пути у

пользователей, находящихся на этом уровне на одно ребро больше. Преимуществом данного подхода является то, что не нужно искать вероятность успешности социоинженерной атаки на каждого пользователя в отдельности, тем самым сложность алгоритма не превышает $O(n \max_{i=1..n}(m_i))$, формула, где n – количество пользователей в системе, а m_i – количество межличностных связей у пользователя i. Недостаток данного подхода заключается в том, что подход аппроксимирует вероятность, а не считает её точно. То есть не учитывает варианты атаки на пользователя через пользователей с уровней ниже. Эмпирически было доказано, что такие цепочки в подавляющем большинстве случаев ничтожно малы, по сравнению с цепочками меньшей длинны до данного пользователя и почти не меняют значение вероятности успешности атаки.

Третий способ заключается в некотором изменении второго. Будем также рассматривать обход в ширину, но считать будем вероятность успешности социоинженерной атаки на пользователя, от сотрудников с меньшими номерами. Причем нумеровать пользователей будем в порядке их просмотра и расчета их вероятностей. Способ отличается от второго тем, что не рассматриваются излишние пути, как, например, 1-3-4-3 (рис. 1). Недостатком данного подхода является то, что он так же не точен, а лишь приближенно вычисляет значения. В том числе не рассматриваются еще и пути от большего номера к меньшему.

Описание программного продукта. Разработанный программный комплекс работает напрямую с базой данных. Продукт имеет текстовый интерфейс для вывода результатов вычисления. Так же есть возможность для добавления в будущем и графического интерфейса, такого как построение гистограмм в Microsoft Excel. В главном окне можно выбрать точку входа социоинженерной атаки и в текстовом окне отобразится информация о ходе атаки и ее результатах, рис. 2.

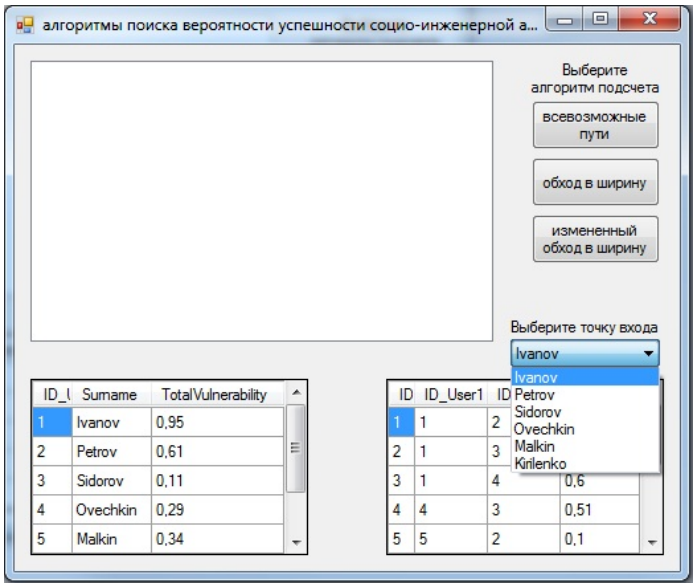


Рис. 2 Фрагмент основного меню

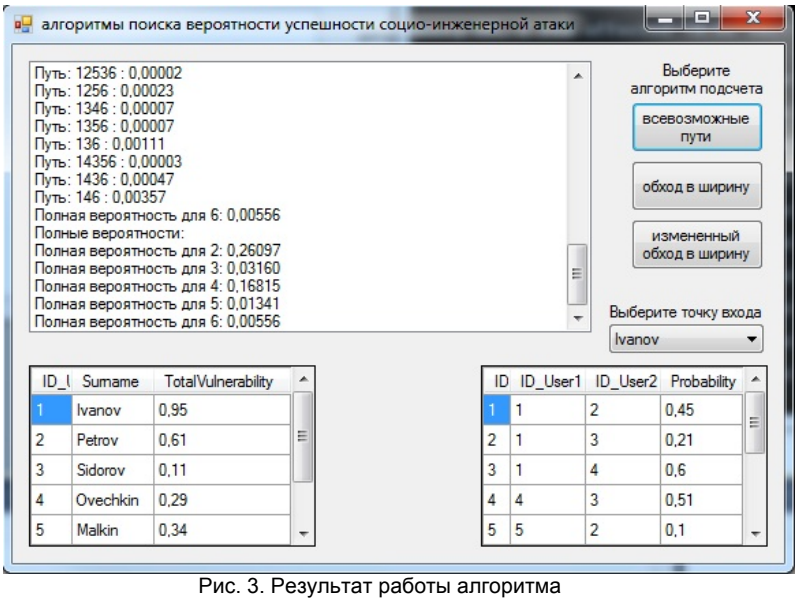


Рис. 3. Результат работы алгоритма

Программный продукт предназначен для анализа защищенности пользователей информационных систем с учетом угроз социоинженерных атак. Целесообразно применять данный продукт на стадии проектирования информационной системы с целью выбрать подходящий алгоритм расчета атакоустойчивости системы на основе ее размера и необходимой точности.

Заключение. В статье представлен прототип программного продукта, предназначенный для анализа защищенности пользователей информационных систем от социоинженерных атакующий воздействий злоумышленника. В программном продукте реализован ряд близких по принципу работы алгоритмов, но существенно различающихся в быстродействии.

СПИСОК ЛИТЕРАТУРЫ

1. Суворова А.В., Тулупьев А.Л., Пащенко А.Е., Тулупьева Т.В., Красносельских Т.В. Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании. № 4. 2010. С. 30–38.
2. Тулупьев А.Л., Азаров А.А., Пащенко А.Е. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2 (13). С. 143–155.
3. Чалдини Р. Психология влияния. Убеждай, воздействуй, защищайся. — СПб.: Питер, 2010. — 336 с.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

Бачило И.Л., Вус М.А., Макаров О.С., Юсупов Р.М.
СОТРУДНИЧЕСТВО РОССИЙСКИХ И БЕЛОРУССКИХ УЧЕНЫХ В РАЗРАБОТКЕ МОДЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МПА СНГ 5

Бобонец С.А, Кузнецов И.В., Примакин А. И.
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА И БЕЗОПАСНОСТИ СПЕЦПОДРАЗДЕЛЕНИЙ СИЛОВЫХ ВЕДОМСТВ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ В СИСТЕМАХ ИНЖЕНЕРНОЙ РАЗВЕДКИ МЕТОДА СОГЛАСОВАНИЯ СЛУХОВОГО АНАЛИЗАТОРА ОПЕРАТОРА С АКУСТИЧЕСКИМ КАНАЛОМ 9

Жигадло В.Э.
АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕРРИТОРИЯМИ «БЕЗОПАСНЫЙ ГОРОД» 13

Кононов О.А., Кононова О.В., Попенко Н.В.
ИНФОРМАТИЗАЦИЯ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ 24

Парфенов Н.П.
ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – ЭФФЕКТИВНЫЙ МЕТОД ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД 29

Шалагинова О.Б.
ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 32

Советов Б.Я., Колбанев М.О., Татарникова Т.М.
РАЗВИТИЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ И БЕЗОПАСНОСТЬ 33

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ 39

Зеленцов В.А., Ковалев А.П., Кожанов А.Н., Пиманов И.Ю., Потрясаев С.А., Скобцов В.Ю.
ИНТЕГРАЦИЯ ПОДСИСТЕМ И СЕРВИСОВ ДОСТУПА К РЕЗУЛЬТАТАМ КОСМИЧЕСКОГО МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ 39

Калачева С.Б.
МЕТОДИКА ГАРАНТИРОВАННОГО ВЫПОЛНЕНИЯ ЗАДАЧ ПРИ РАССТАНОВКЕ ПО ПРОЦЕССОРАМ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ 44

Микони С.В.
ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ СИСТЕМАТИЗАЦИИ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОГО ВЫБОРА НА КОНЕЧНОМ МНОЖЕСТВЕ АЛЬТЕРНАТИВ 48

Никифоров В.В. .....
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИСПОЛНЕНИЯ ПРОГРАММНЫХ КОМПЛЕКСОВ ДЛЯ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ 53

Олимпиев А.А.
ВЫЧИСЛИТЕЛЬНЫЙ ФОРМАЛИЗМ СИНТАКСИЧЕСКИ ВАРИАНТНОЙ СИСТЕМЫ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО МОНИТОРИНГА ГЕТЕРОГЕННЫХ СЕТЕЙ СВЯЗИ 57

Вашко В.Ю., Ковалев А.П., Семенков О.И., Зеленцов В.А., Потрясаев С.А., Соколов Б.В.
МНОГОКРИТЕРИАЛЬНОЕ ПЛАНИРОВАНИЕ МОДЕРНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ УНАСЛЕДОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ 62

Федорченко Л.Н.
SYNGT: ПРИМЕНЕНИЕ АТРИБУТОВ 68

Чуднов А.М., Сапунова Л.П.
ОБ АДАПТИВНЫХ АЛГОРИТМАХ ППРЧ В УСЛОВИЯХ СЛУЧАЙНЫХ И ПРЕДНАМЕРЕННЫХ ПОМЕХ 73

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ 79

Богатырев В.А., Богатырев А.В., Богатырев С.В.
ОПТИМАЛЬНОЕ РЕЗЕРВИРОВАНИЕ ОТКАЗОУСТОЙЧИВОЙ ДРЕВОВИДНОЙ СЕТИ 79

Брунилин А.А.
ПЕРСПЕКТИВЫ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ДЛЯ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ..... 82

Верзун Н.А.
МНОГОКРИТЕРИАЛЬНЫЙ ВЫБОР СТРУКТУРЫ ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ 87

Верзун Н.А.
ОБМЕН И УДАЛЕННАЯ ОБРАБОТКА ИНФОРМАЦИИ В ДВУХУРОВНЕВОЙ АССОЦИАЦИИ СИСТЕМ МНОЖЕСТВЕННОГО ДОСТУПА..... 91

Воробьева А.А.
МОДЕЛЬ АВТОРА И ТЕКСТА В РЕШЕНИИ ЗАДАЧИ ИДЕНТИФИКАЦИИ АВТОРА АНОНИМНЫХ СООБЩЕНИЙ В СЕТИ ИНТЕРНЕТ..... 95

Горелик С.Л., Ляпер В.С.
ДИСТАНЦИОННАЯ РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И ДОКУМЕНТОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ 99

Дойникова Е.В., Котенко И.В.
АНАЛИЗ И ПРИМЕНЕНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ В SIEM-СИСТЕМАХ НА ОСНОВЕ ГРАФОВ АТАК И ЗАВИСИМОСТЕЙ СЕРВИСОВ..... 104

Ковалев И.Г.
МЕТОД КОМПОЗИЦИИ ЧАСТНЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ В ЗАДАЧЕ ТИПИЗАЦИИ СИТУАЦИЙ В УПРАВЛЕНИИ ТЕЛЕКОММУНИКАЦИОННЫМИ СИСТЕМАМИ..... 112

Ковалев И.Г., Потемкин Э.К.
ЭВРИСТИЧЕСКАЯ ДЕКОМПОЗИЦИЯ ЗАДАЧИ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СИСТЕМАМИ НА ОСНОВЕ МЕТОДА СИТУАЦИОННОГО УПРАВЛЕНИЯ 117

Мошак Н.Н., Иванов В.И.
ПРЕДОСТАВЛЕНИЕ СЕРВИСОВ БЕЗОПАСНОСТИ В ПАКЕТНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ В ТЕРМИНАХ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ 121

Левкин И.М., Галкова Е.А.
РАСПРЕДЕЛЕНИЕ СИЛ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ДИНАМИЧЕСКОЙ СРЕДЫ ИНФОРМАЦИОННЫХ УГРОЗ..... 125

Паращук И.Б.
СЕТЕВОЙ МОНИТОРИНГ КАК КЛЮЧЕВОЙ ЭТАП ПОДГОТОВКИ И ПРИНЯТИЯ РЕШЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 130

Салухов В.И., Шевченко О.И.
УПРАВЛЕНИЕ РИСКАМИ НА РАЗЛИЧНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 133

Татарникова Т.М. Яготинцева Н.В.
ИНТЕГРАЦИЯ ОБРАЗЦОВ РАДИОЭЛЕКТРОННОГО ВООРУЖЕНИЯ НА ОСНОВЕ ИНФОРМАЦИОННОЙ ТРАНСПОРТНОЙ СЕТИ КОРАБЛЯ 148

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ..... 152

Александрова Е.Б., Кузнецова Е.А.
ОТЗЫВ И ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ В РЕШЕТОЧНОЙ VLR-СХЕМЕ ГРУППОВОЙ ПОДПИСИ 152

Алексеев А.В., Воробьев В.И.
ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО: 20 ЛЕТ КОНЦЕПТУАЛЬНОГО И ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ 153

Афанасьев С.В.
ОНТОЛОГИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ОБЛАЧНЫХ СЕРВИСОВ 160

Блюм В.С.
ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИОЛОГИЧЕСКИХ СИСТЕМАХ..... 162

Горбачев И.Е., Якунин В.И.,
ПРИНЦИПЫ СЕМИОТИЧЕСКОГО МОДЕЛИРОВАНИЯ КОНФЛИКТУЮЩИХ СИСТЕМ В ПРИЛОЖЕНИИ К ЗАДАЧЕ ВНЕШНЕГО ПРОЕКТИРОВАНИЯ ПРОАКТИВНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 170

Головкин Ю.Б., Гусаренко А.С.
SMARTY-ОБЪЕКТЫ В СИТУАЦИОННО-ОРИЕНТИРОВАННЫХ БАЗАХ ДАННЫХ..... 176

Головкин Ю.Б.,Ярцев Р.А., Газетдинова С.Г.,Арсланова А.Р., Давлетов Г.Б.
ДИНАМИЧЕСКАЯ МОДЕЛЬ ДИСКРЕТНЫХ ПРОЦЕССОВ С УЧЕТОМ ПРЕДЫСТОРИИ..... 178

Дубровская В.А.
АНАЛИЗ СОСТОЯНИЯ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ОТЕЧЕСТВЕННЫХ СИСТЕМАХ ЗАЩИТЫ И ИХ СРАВНЕНИЕ 180

Золотарева К.Н.
ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ЛАЗЕРНЫМ МИКРОФОНАМ 185

Ковалев И.Г.
АНАЛИЗ РЕАЛИЗАЦИЙ ПРОЦЕДУР ТИПИЗАЦИИ И ЭКСТРАПОЛЯЦИИ СИТУАЦИЙ В АЛГОРИТМЕ КЛАССИФИКАЦИИ СИТУАЦИЙ 187

Кононов О.А., Кононова О.В.
ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ В ИТ ИНФРАСТРУКТУРЕ ВУЗА И УГРОЗЫ БЕЗОПАСНОСТИ 191

Копыльцов А.А.
ОЦЕНИВАНИЕ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ 194

Копыльцов А.В.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ЛОКАЛЬНОЙ РЕГУЛЯЦИИ КРОВОТОКА..... 199

Марков А.С., Фадин А.А.
РЕАЛИЗАЦИОННЫЕ ОСНОВЫ СИГНАТУРНО-ЭВРИСТИЧЕСКОГО АНАЛИЗА БЕЗОПАСНОСТИ ПРОГРАММ 204

Пойманова Е.Д.
ОРГАНИЗАЦИЯ МЕТАДАННЫХ ПРИ ДЛИТЕЛЬНОМ ХРАНЕНИИ ИНФОРМАЦИИ 206

Пойманова Е.Д.
УСЛУГИ ДЛИТЕЛЬНОГО ХРАНЕНИЯ ДАННЫХ..... 209

Сенцова А.Ю., Машкина И.В.
ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ 214

Сухопаров М.Е.
РАССЧЕТ ИНФОРМАТИВНОСТИ ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ, ОСНОВАННОГО НА КОРТЕЖЕ ЛИНГВИСТИЧЕСКИХ ПРИЗНАКОВ 218

Татарникова Т.М. Яготинцева Н.В.
ЗАЩИТА РЕСУРСОВ ГИС..... 222

Харинов М.В., Заболотский В.П.
ЦЕЛОЧИСЛЕННАЯ ОЦЕНКА КОЛИЧЕСТВА ИНФОРМАЦИИ В ЗАДАЧАХ СТЕГАНОГРАФИИ И РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ..... 227

Шишкин В.М., Абросимов И.К.
ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ РАЗВИТИЯ ИКТ И ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ..... 230

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 235

Березин А.Н.
ОБЩИЕ ВОПРОСЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СХЕМ ПО СОСТАВНОМУ МОДУЛЮ 235

Березин А.Н., Демьянчук А.А., Рыжков А.В.
ПРОТОКОЛЫ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, ИСПОЛЬЗУЮЩИЕ АЛГОРИТМЫ ОТКРЫТОГО ШИФРОВАНИЯ 240

Богатырев В.А., Богатырев А.В.
ОТКАЗОУСТОЙЧИВОСТЬ КОНФИГУРАЦИЙ ЦЕНТРОВ ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ 246

Богатырев В.А., Богатырев А.В., Богатырев С.В.
ОРГАНИЗАЦИЯ МЕЖМАШИННОГО ОБМЕНА В КОМПЬЮТЕРНЫХ СИСТЕМАХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ 250

Емельянов А.А.
ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ВНУТРИКОРПОРАТИВНЫХ ПОЛИТИК БЕЗОПАСНОСТИ НА ПРИМЕРЕ МАЛОГО ПРЕДПРИЯТИЯ 253

Золотарева Е.Н.
СИСТЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ КАК СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 255

Канев А.Н.
АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТРИК 257

Касаткин В.В., Колбанев М.О., Татарникова Т.М.
ПРЕДМЕТНАЯ ОБЛАСТЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 260

Блюм В.С., Заболотский В.П.
СОЦИАЛЬНАЯ ИММУННАЯ СИСТЕМА И ИММУНОКОМПЬЮТИНГ 264

Копыльцов А.А.
СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ИЗВЛЕКАЕМОЙ СПЕЦИАЛЬНЫМ ОБРАЗОМ ИНФОРМАЦИИ 272

Кудрявцева К.А.
АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ВОЛОКОННО-ОПТИЧЕСКОГО КАНАЛА СВЯЗИ ОТ УГРОЗЫ ПЕРЕХВАТА ТРАФИКА 277

Молдовян А.А., Молдовян Н.А., Касаткин В.В.
ВОПРОСЫ И РЕШЕНИЯ СОВРЕМЕННОЙ КРИПТОГРАФИИ ДЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ 281

Молдовян А.А., Березин А.Н., Михтеев М.С.
ОТРИЦАЕМОЕ ШИФРОВАНИЕ НА ОСНОВЕ СТАНДАРТНОЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ 285

Молдовян А.А., Молдовян Н.А.
ОТРИЦАЕМОЕ ШИФРОВАНИЕ: АЛГОРИТМЫ, ПРОТОКОЛЫ И ПРИМЕНЕНИЯ 289

Молдовян А.А., Ковцур М.М.
ОЦЕНКА СКОРОСТНЫХ ХАРАКТЕРИСТИК РЕАЛИЗАЦИИ АТАКИ ТИПА ПЕРЕБОР ПАРОЛЯ НА IP-АТС ПРИ ИСПОЛЬЗОВАНИИ FAIL2BAN 294

Насретдинова Д.Р.
УНИЧТОЖЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ 299

Нурдинов Р.А.
ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ДЕСТРУКТИВНЫХ СОСТОЯНИЙ И ПЕРЕХОДОВ 301

Петрук Т.Н.
ИЗГИБ ОПТИЧЕСКОГО ВОЛОКНА КАК ОДИН ИЗ СПОСОБОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ 306

Солодянников А.В., Пилипов М.В., Парамонов А.В.
ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРИМЕТРА АВТОМАТИЗИРОВАННЫХ КАРТОГРАФИЧЕСКИХ СИСТЕМ 309

Ральникова Н.С.
ОПТИЧЕСКОЕ ТУННЕЛИРОВАНИЕ КАК МЕТОД ФОРМИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ 310

Сорокин И.В., Копыльцов А.В.
МОДЕЛИ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ НА ОСНОВЕ ЭНТРОПИЙНЫХ ХАРАКТЕРИСТИК 313

Федотова А.В., Волков А.В., Тарасов В.Б.
ОТ КЛАССИЧЕСКИХ К МНОГОАГЕНТНЫМ СИСТЕМАМ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ 316

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И БИЗНЕСЕ 320

Богатырев В.А., Богатырев А.В.
ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИОННЫХ УСЛУГ РЕАЛЬНОГО ВРЕМЕНИ В УСЛОВИЯХ ОШИБОК, ОТКАЗОВ И ДИСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ 320

Васькова А.В., Михайличенко Е.М.
ТРАНСПОРТНЫЙ ФАКТОР КАК ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 324

Верзун Н.А., Колбанев М.О.
НЕКОТОРЫЕ АСПЕКТЫ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 327

Колбанев М.О., Микадзе С.Ю., Татарникова Т.М.
ФИЗИЧЕСКИЙ ОБЪЕМ БАЗОВЫХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ 330

Коршунов И.Л., Суворова О.В.
РОЛЬ И МЕСТО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В НАПРАВЛЕНИИ ПОДГОТОВКИ 080101.65 «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ» 335

Левкина С.В., Микадзе С.Ю.
ВНЕШНЕЭКОНОМИЧЕСКАЯ ЭКСПАНСИЯ: ПРИЗНАКИ СОСТОЯНИЯ 337

Маркелов К.С., Нечаев В.В.
БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 342

Марков А.С., Фадин А.А., Цирлов В.Л., Рауткин Ю.В.
О ЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ 345

Мошак Н.Н.
СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕРРИТОРИАЛЬНЫХ УЧРЕЖДЕНИЯХ БАНКА РОССИИ 347

Пичугин Ю.А., Кондрашков А.В.
СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И РИСКА НА ОСНОВЕ АЛЬТМАНОВСКОГО ПОДХОДА 352

Попова Е.В.
МНОГОКРИТЕРИАЛЬНЫЙ ОПТИМИЗАЦИОННЫЙ ВЫБОР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЙ 357

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ 361

Ерохин А.В., Ерохин В.И.
ЭФФЕКТИВНЫЙ МЕТОД ГРУППОВОЙ НАВИГАЦИИ, ОСНОВАННЫЙ НА МОДИФИЦИРОВАННОМ АЛГОРИТМЕ A* 361

Ханыков И.Г.
СОПОСТАВЛЕНИЕ ДВУХ МЕТОДОВ АВТОМАТИЧЕСКОЙ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ 366

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 371

Устинов И.А.
ПРОБЛЕМЫ, ЦЕЛИ И ЗАДАЧИ УНИФИКАЦИИ КЛЮЧЕВЫХ СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКИХ ИНФРАСТРУКТУР 371

Устинов И.А., Игумнов В.В.
ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР 373

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ 377

Государев И.Б.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ: СЕМИОТИЧЕСКИЙ ПОДХОД 377

Дмитриева А.В., Ключарев А.А., Степанов А.Г.
ОБЗОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ В УЧЕБНОМ ПРОЦЕССЕ КАФЕДРЫ УНИВЕРСИТЕТА 380

Колоколова Л.П.
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАТИВНЫХ ТЕХНОЛОГИЙ НА ЗАНЯТИЯХ ПО РУССКОМУ ЯЗЫКУ 386

Лаптев В.В., Носкова Т.Н., Флегонтов А.В., Гавронская Ю.Ю., Пиотровская К.Р.
ПОИСК СТРАТЕГИЙ КОНВЕРГЕНЦИИ НАУКИ ВЫСОКИХ ТЕХНОЛОГИЙ И ОБРАЗОВАТЕЛЬНЫХТЕХНОЛОГИЙ НОВОГО ТИПА 389

Моглан Д.В., Абрамян Г.В.,
ОПЫТ ИСПОЛЬЗОВАНИЯ ОБРАЗОВАТЕЛЬНЫХ СЕТЕВЫХ СООБЩЕСТВ НА ОСНОВЕ БЛОГОВ ПРИ ОБУЧЕНИИ СТУДЕНТОВ ДИСЦИПЛИНЕ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» 393

Степанов А.Г., Космачев В.М., Шкиртиль М.А.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО БОРЬБЫ С ПАРАЛЛЕЛЬНЫМ РЫНКОМ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ 398

Степанов А.Г., Карасева Е.И., Зуева Н.В., Москалева О.И.
СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБУЧЕНИИ БУДУЩИХ ЭКОНОМИСТОВ 401

Степанов А.Г., Семенова Е.Г., Фролова Е.А.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ПОВЫШЕНИИ КАЧЕСТВА ОЦЕНКИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ 404

Тумалева Е.А.
ВИРТУАЛЬНАЯ СОСТАВЛЯЮЩАЯ НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВУЗА 4088

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ 414

Абрамян Г.В.
РИСКИ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ НА ПЛАТФОРМЕ WINDOWS НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ РОССИЙСКОЙ ФЕДЕРАЦИИ 414

Буйневич М.В., Бучкова Е.С., Быстрова О.Д.
ПЕРСПЕКТИВЫ РАЗРАБОТКИ И АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ 416

Солодянников А.В., Пилипов М.В., Федоров Д.Ю.
ТРЕБОВАНИЯ К АККРЕДИТАЦИИ КОМПАНИЙ, ЗАНИМАЮЩИХСЯ АУДИТОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 418

Бобонец С.А., Куватов В.И., Примакин А.И.
К ВОПРОСУ ПРИМЕНЕНИЯ СТАТИСТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ ЗНАНИЙ КУРСАНТОВ ПО УЧЕБНЫМ ДИСЦИПЛИНАМ НАПРАВЛЕНИЯ ПОДГОТОВКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» В УЧЕБНЫХ ЗАВЕДЕНИЯХ СИСТЕМЫ МВД РОССИИ 420

Залещанский Б.Д., Свиридов А.П., Павлова О.А., Шалобина Е.А.
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СОЦИО-ТЕХНИЧЕСКИХ СИСТЕМ ЭКОНОМИЧНЫМИ СТРАТЕГИЯМИ УПРАВЛЕНИЯ ПОДГОТОВКОЙ ПЕРСОНАЛА 425

Куватов В.И., Примакин А.И., Синещук Ю.И.
ПРИМЕНЕНИЕ МОДУЛЬНОГО ПРИНЦИПА, КАК ФОРМЫ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ПОДГОТОВКЕ КУРСАНТОВ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПО СПЕЦИАЛЬНОСТИ 090915.65 – «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ» 429

Пуха Г.П.
СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ – ИННОВАЦИОННОЕ НАПРАВЛЕНИЕ ИССЛЕДОВАНИЙ И ПОДГОТОВКИ СПЕ-ЦИАЛИСТОВ ИТ 432

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗДРАВООХРАНЕНИИ 438

Бланк М.А., Бланк О.А., Мясникова Е.М., Рудницкий С.Б., Денисова Д.М.
ЗАКОНОМЕРНОСТЬ РАСПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ ТРЕВОЖНОСТИ ВЗРОСЛОГО ЧЕЛОВЕКА 438

Блюм В.С.
СОБЫТИЙНАЯ МОДЕЛЬ БАЗЫ ДАННЫХ ИНТЕГРИРОВАННЫХ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ ДЛЯ РЕШЕНИЯ ЗАДАЧ МЕДИЦИНСКОЙ СТАТИСТИКИ 442

Блюм В.С., Заболотский В.П.
КЛАССИФИКАЦИЯ ПРОГРАММНЫХ АГЕНТОВ ДЛЯ РАННЕГО ОБНАРУЖЕНИЯ ДЕФЕКТОВ ОКАЗАНИЯ МЕДИЦИНСКОЙ ПОМОЩИ ПО ДАННЫМ ИНТЕГРИРОВАННОЙ ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТЫ 451

Инкин В.А., Делакова Е.А.
СОЗДАНИЕ СТРУКТУРЫ ИНТЕЛЛЕКТУАЛЬНОЙ ЭКСПЕРТНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ АНАЛИЗА МЕДИКО-БИОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ 459

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ 464

Ходаков В.Е., Соколова Н.А., Антипенко И.В., Бабина О.В.
ОЦЕНИВАНИЕ РАЗВИТИЯ ОДНОГО КЛАССА СЛОЖНЫХ СИСТЕМ С УЧЁТОМ ПРИРОДНО-КЛИМАТИЧЕСКИХ ФАКТОРОВ 464

Михайлов В.В., Переварюха А.Ю., Соловьева И.В.
АНАЛИЗ ПРОБЛЕМ ИХТИОЦЕНОЗА МОРСКОЙ ЭКОСИСТЕМЫ НА ОСНОВЕ КОГНИТИВНОЙ ГРАФОВОЙ МОДЕЛИ 469

Переварюха А.Ю., Мосейко А.Г.
ФЕНОМЕНОЛОГИЧЕСКАЯ МОДЕЛЬ ПОВТОРЯЮЩИХСЯ ВСПЫШЕК ЧИСЛЕННОСТИ ВРЕДИТЕЛЕЙ ЛЕСА 474

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 480

Абрашкин А.В., Саушев А.В.
ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОЦЕССА СУДОПРОПУСКА ПУТЕМ УСТАНОВКИ НА СУДОХОДНЫЕ ШЛЮЗЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ 480

Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В.
РАНГОВАЯ ПАРТНЕРСКАЯ СЕРТИФИКАЦИЯ КАЧЕСТВА: КОНЦЕПЦИЯ, ТЕОРИЯ, ПРАКТИКА 485

Алексеев А.В., Тюрин И.С.
ТЕХНОЛОГИИ МОНИТОРИНГА И УПРАВЛЕНИЯ ЗАЩИЩЕННОСТЬЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И ИНФРАСТРУКТУРЫ 491

Алексеев С.А., Алексеева Е.К.
АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ ПРИ ТРЕНАЖЕРНОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ВМФ 497

Баркова Н.А., Грищенко Д.В.
НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ ТЕХНОЛОГИЙ ДИАГНОСТИКИ РОТОРНОГО ОБОРУДОВАНИЯ 503

Белоусов И.В.
ФОРМИРОВАНИЕ ОПТИМАЛЬНОГО РАСПИСАНИЯ ДВИЖЕНИЯ СУДОВ ЧЕРЕЗ ШЛЮЗ ПО КРИТЕРИЮ МИНИМУМА ВРЕМЕНИ ПРОСТОЯ 508

Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И.
ОПЫТ ОРГАНИЗАЦИИ РАНГОВОЙ ПАРТНЕРСКОЙ СЕРТИФИКАЦИИ КАЧЕСТВА ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ 511

Бориев З.В., Соколов С.С.
БИОМЕТРИЧЕСКИЕ МЕТОДЫ АУТЕНТИФИКАЦИИ: НАСТОЯЩЕЕ И БУДУЩЕЕ 517

Волков В.И., Тычинин И.Ю., Алексеев А.В.
АНАЛИЗ СИСТЕМНЫХ АСПЕКТОВ УПРАВЛЕНИЯ РАЗВИТИЕМ КРИТИЧЕСКИХ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 520

Грищенко Д.В.
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ОПЕРАТИВНОГО ДИАГНОСТИРОВАНИЯ СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ 526

Егоров А.Н., Кузнецов В.А., Назаргулов И.А.
ПРОГРАММНАЯ ОБОЛОЧКА РАСПАРАЛЛЕЛИВАНИЯ ДЛЯ ВОССТАНОВЛЕНИЯ ДОСТУПА К ДАННЫМ 530

Некрасова А.А., Соколов С.С.
О НЕКОТОРЫХ МЕТОДАХ ИСПОЛЬЗОВАНИЯ МОДЕЛЕЙ ПЕРКОЛЯЦИИ ДЛЯ МОДЕЛИРОВАНИЯ ПРОЦЕССА В ИНФОРМАЦИОННЫХ СЕТЯХ 534

Поленин В.И., Ребенок Ю.С.
СЕТЕВОЕ ПЛАНИРОВАНИЕ И УПРАВЛЕНИЕ ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ СОВЕРШЕНСТВОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СУДАМИ И БОРЬБОЙ ЗА ЖИВУЧЕСТЬ 536

Поленин В.И., Можаев А.С., Можаева И.А.
КОНЦЕПЦИЯ ПОСТРОЕНИЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ ПОДДЕРЖКИ МАКРОУРОВНЕВОГО ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ВЫПОЛНЕНИЕМ ЗАДАЧ С ПРИМЕНЕНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ 540

Приходько В.М., Приходько И.В.
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ХАРАКТЕРИСТИК СУШКИ СУДОВЫХ АСИНХРОННЫХ ДВИГАТЕЛЕЙ 545

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 550

Кефели И.Ф., Меркулов А.Л.
ГЛАВНАЯ ПРИЧИНА РАСПАДА СССР 550

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ 554

Азаров А.А., Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В.
ПРОТОТИП КОМПЛЕКСА ПРОГРАММ ДЛЯ АНАЛИЗА ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫЙ НА ОСНОВЕ АЛГОРИТМОВ ОБХОДА ГРАФОВ СОЦИАЛЬНЫХ СВЯЗЕЙ ПОЛЬЗОВАТЕЛЕЙ 554

ОГЛАВЛЕНИЕ 558

CONTENTS

Bachilo I.L., Vus M.A., Makarov O.S., Yusupov R.M.,
COOPERATION BETWEEN RUSSIAN AND BELARUSIAN SCIENTISTS DEVELOP MODEL LEGISLATION IN THE FIELD OF INFORMATION SECURITY FOR CIS INTERPARLIAMENTARY 5

Bobonets S.A., Kuznetsov I.V., Primakin A.I.
PROVIDING INFORMATION SUPERIORITY AND SAFETY OF SPECIAL FORCES OF POWER DEPARTMENTS BY MEANS OF APPLICATION IN SYSTEMS OF ENGINEERING INVESTIGATION OF THE METHOD OF COORDINATION OF THE ACOUSTIC ANALYZER OF THE OPERATOR WITH THE ACOUSTIC CHANNEL 9

Zhigadlo V.
AUTOMATED INFORMATION MANAGEMENT SYSTEM TERRITORY OF THE "SAFE CITY" 13

Kononov O., Kononova O., Popenko N.
INFORMATIZATION AND LEGAL SUPPORT 25

Parfenov N.
DEPERSONALIZATION OF PERSONAL INFORMATION – AN EFFECTIVE METHOD OF PROTECTION OF PERSONAL INFORMATION OF STAFF OF DEPARTMENT OF INTERNAL AFFAIRS 29

Shalaginova O.B.
TECHNOLOGY OF INFORMATION SECURITY IN LAW ENFORCEMENT 32

Sovetov B., Kolbanev M., Tatarnikova T.
TECHNOLOGY INFORMATION COMMUNICATION AND SECURITY 33

Zelentsov V., Kovalev A., Kojanov A., Pimanov I., Potryasaev S., Skobtsov V.
INTEGRATION OF SUBSYSTEMS AND SERVICES FOR ACCESS TO THE RESULTS OF EMERGENCIES SPACE MONITORING AND FORECASTING[1] 39

Kalacheva S.
METHOD OF THE GARANTEE TASK FULFILING WHEN DISTRIBUTION ON THE PROCESSORS IN THE REAL-TIME APPLICATION 44

Mikoni S.
THEORETICAL JUSTIFICATION OF SYSTEMATIZATION OF METHODS MULTICRITERIA OPTIMIZATION ON A FINITE SET OF ALTERNATIVES 48

Nikiforov V.
SIMULATION OF SOFTWARE APPLICATION EXECUTION IN REAL-TIME SYSTEMS 53

Olimpiev A.
COMPUTATION FORMALISM OF VARIABLE SYNTAX MONITORING SYSTEM WITH SYNTATIC VARIANCE 57

Vashko V., Kovalev A., Semenkov O., Zelentsov V., Potryasaev S. , Sokolov B. .....
MULTICRITERIA PLANNING OF MODERNIZATION AND FUNCTIONING OF THE INHERITED INFORMATION SYSTEM 63

Fedorchenko L.
SYNGT: IMPLEMENTATION OF ATTRIBUTES 68

Chudnov A., Sapunova L.
ON ADAPTIVE ALGORITHMS FHSS UNDER RANDOM AND INTERNIONAL INTERFERENCE 73

Bogatyrev V., Bogatyrev A., Bogatyrev S.
OPTIMAL REDUNDANCY OF FAULT-TOLERANT NETWORK TREE TOPOLOGY 79

Brunilin A.
ONTOLOGICAL APPROACH TO INFORMATION INTERACTION ORGANIZATION OF HETEROGENEOUS AUTOMATED SYSTEMS FOR SPECIAL PURPOSES 83

Verzun N.
MULTICRITERIA CHOICE LAN STRUCTURE COMPANY 88

Verzun N.
EXCHANGE AND REMOTE DATA PROCESSING TWO-TIER ASSOCIATION MULTIPLE ACCESS 91

Vorobeva A.A.
THE AUTHOR AND TEXT MODEL IN THE SOLUTION OF ANONYMOUS MESSAGE AUTHOR IDENTIFICATION TASK IN INTERNET NETWORK 95

Gorelik S., Lyaper V.
REMOTE REGISTRATION OF USERS AND DOCUMENTS IN TELECOMMUNICATION SYSTEMS 99

Doynikova E.V., Kotenko I.V.
ANALYSIS AND APPLICATION OF THE SECURITY METRICS ON THE BASE OF THE ATTACK GRAPHS AND SERVICE DEPENDENCIES GRAPHS FOR THE SIEM SYSTEMS 104

Kovalev I.
THE METHOD OF COMPOSITION INDIVIDUAL PERFORMANCE INDICATORS IN THE TASK TYPING SITUATIONS IN THE MANAGEMENT OF TELECOMMUNICATION SYSTEMS..... 112

Kovalev I., Potemkin E.
HEURISTIC DECOMPOSITION OF THE PROBLEM OF MANAGEMENT OF TELECOMMUNICATION SYSTEMS ON THE BASIS OF SITUATIONAL MANAGEMENT..... 117

Moshak N.N., Ivanov V.I.
SERVICES SECURITY IN MULTI SERVICES COMMUNICATIONS NEWORK IN TERMINUS OF MODEL OPEN SYSTEMS INTERCONNECTED..... 122

Levkin I., Galkova E.
THE DISTRIBUTION OF FORCES AND MEANS OF INFORMATION PROTECTION IN THE CONDITIONS OF DYNAMIC ENVIRONMENT INFORMATION THREATS..... 126

Paraschuk I.
NETWORKING MONITORING AS THE BASIC OF STAGE PREPARATION AND ADOPTION DECIDE AFTER THE CONTROL OF INFORMATION SECURITY OF REGIONAL TELECOMMUNICATION NETWORKS..... 131

Salukhov V., Shevchenko O.
RISK MANAGEMENT AT VARIOUS STAGES THE LIFE CYCLE OF TELECOMMUNICATION SYSTEMS 133

Tatarnikova T., Yagotinceva N.
TECHNOLOGY INFORMATION COMMUNICATION AND SECURITY 148

Alexandrova E., Kuznetsova E.
REVIEWS AND ADDING USERS TO THE VLR-LATTICE CHART GROUP SIGNATURE..... 152

Alekseev A., Vorobiev V.
INFORMATION CONFRONTATION: 20 YEARS OF CONCEPTUAL AND TECHNOLOGICAL DEVELOPMENT..... 153

Afanasyev S.V.
ONTOLOGICAL APROACH TO DEFINE CLOUD SRVICES 160

Blum V.
FEATURES INFORMATION SECURITY BIOLOGICAL SYSTEMS..... 162

Gorbachev I., Yakunin V.
PRINCIPLES OF CONFLICT OF MODELING SEMIOTIC AS APPLIED TO EXTERNAL DESIGN PROACTIVE INFORMATION SECURITY SYSTEMS 170

Golovkin Y., Gusarenko A.
SMARTY-OBJECTS IN SITUATION-ORIENTED DATABASES 176

Golovkin Y., Yarchev R., Gazetdinova S., Arslanova A., Davletov G.
DYNAMIC MODEL DISCRETE PROCESSES WITH HISTORY 178

Dubrovskaya V.
ANALYSIS OF THE USED INFORMATION SECURITY FEATURES IN DOMESTIC PROTECTION SYSTEMS AND THEIR COMPARING 180

Zolotareva K.
ORGANIZATIONAL METHODS TO COUNTERACT LASER MICROPHONES 185

Kovalev I.
ANALYSIS IMPLEMENTATIONS PROCEDURES TYPING AND EXTRAPOLATION SITUATIONS IN THE ALGORITHM OF CLASSIFICATION SITUATIONS 188

Kononov O., Kononova O.
VIRTUALIZATION TECHNOLOGIES IN THE IT INFRASTRUCTURE OF THE UNIVERSITY AND THE SECURITY THREATS 191

Kopyltsov A.
SAFETY EVALUATION ENTERS WEAKLY FORMALIZED INFORMATION 194

Kopyltsov A.
INFORMATION SECURITY IN LOCAL BLOOD FLOW REGULATION 199

Markov A. S., Fadin A. A.
IMPLEMENTAL BASICS OF SIGNATURE-HEURISTIC ANALYSIS OF SECURITY SOFTWARE 204

Poymanova E.
ORGANIZATION OF METADATA WITH LONG-TERM INFORMATION STORAGE 206

Poymanova E.
SERVICES OF LONG TERM STORAGE 209

Sentsova A., Mashkina I.THE ARTIFICIAL NEURALNETWORK APPLICATION FOR SECURITY RISK ASSESSMENT IN CLOYD COMPUTING SYSTEMS 215

Sukhoparov M.E.
EVALUATION OF INFORMATIVE OF LINGUISTIC USER PROFILE 218

Tatarnikova T., Yagotinceva N.
RESOURCE PROTECTION GIS 222

Kharinov M.V., Zabolotsky V.P.
INTEGER ESTIMATION OF INFORMATION QUANTITY IN STEGANOGRAPHY AND IMAGE RECOGNITION TASKS 227

Shishkin V.M., Abrosimov I.K.
DYNAMIC MODEL OF INTERACTION SYSTEM OF IT DEVELOPMENT AND NATIONAL SECURITY ENSURING 231

Berezin A.
GENERAL ITEMS ON DESIGNING THE COMPOSITE-MODULO CRYPTOSCHEMES 235

Berezin A., Dem'janchuk Anna, Rizhkov A.
ZERO KNOWLEDGE PROTOCOLS BASED ON THE PUBLIC ENCRYPTION ALGORITHMS 240

Bogatyrev V., Bogatyrev A.
FAILOVER CONFIGURATION DATA CENTERS 246

Bogatyrev V., Bogatyrev A., Bogatyrev S.
ORGANIZATION OF SAFE INTERCOMPUTER EXCHANGE IN COMPUTER SYSTEMS 250

Emelyanov A.
PRACTICAL IMPLEMENTATION OF SECURITY POLICY IN SMALL BUSINESS CASE 253

Zolotareva E.N.
CONTROL SYSTEM PRIVILEGED USERS AS A MODERN MEANS OF INFORMATION PROTECTION 255

Kanev A.
INFORMATION SYSTEM VULNERABLITY ANALYSIS BASED ON METRICS 258

Kasatkin V., Kolbanev M., Tatarnikova T.
THE SUBJECT AREA OF INFORMATION INTERACTION 260

Blum V., Zabolotski V.
SOCIAL IMMUNE SYSTEM AND IMMUNOCOMPUTING 265

Kopyltsov A.A.
THE SAVE OF CONFIDENTIALITY DATA IN DECISION SUPPORT BASED ON EXTRACTS SPECIALLY INFORMATION 273

Kudriavtseva K.
PROTECTION ASSAY FIBER-OPTIC LINK FROM THE THREAT OF INTERCEPT TRAFFIC 277

Moldovyan A.A., Moldovyan N.A., Kasatkin V.V.
QUESTIONS AND SOLUTIONS OF MODERN CRYPTOGRAPHY FOR COMPUTER SYSTEMS 281

Moldovyan A.A., Berezin A.N., Mihteev M.S.
BI-DENIABLE PUBLIC-KEY ENCRYPTION BASED ON STANDARD PKI 286

Moldovyan A.A., Moldovyan N.A.
DENIABLE ENCRYPTION: MODERN ALGORITHMS AND APPLICATIONS 289

Moldovyan A.A., Kovtsur M.M.
EVALUATION OF SPEED CHARACTERISTICS OF BRUTE FORCE
PASSWORD ATTACK TO IP-PBX WHEN USING FAIL2BAN 294

Nasretdinova D.R.
CONFIDENTIAL DOCUMENT DESTRUCTION 299

Nurdinov R.
INFORMATION SYSTEM SECURITY RISK ASSESSMENT BASED ON STATES
AND TRANSITIONS MODEL 301

Petruk T.
BENDING THE OPTICAL FIBER AS ONE OF THE WAYS OF GETTING INFORMATION 307

Solodyannikov A., Pilipov M., Paramonov A.
PERIMETER PROTECTION IN AUTOMATED MAPPING SYSTEMS 309

Ralnikova N.
OPTICAL TUNNELING AS A METHOD OF FORMING A CHANNELS OF INFORMATION LEAKEGE,
TRANSMITTED ON FIBER-OPTICAL COMMUNICATION LINES 311

Sorokin I.V., Kopyltsov A.V.
MODEL OF MALWARE RECOGNITION BASED ON ENTROPY FEATURES 313

Fedotova A. V., Volkov A. V., Tarassov V. B.
FROM THE CLASSICAL TO MULTI-AGENT SYSTEMS OF CORPORATE DATA PROTECTION 316

Bogatyrev V., Bogatyrev A.
ECONOMIC EFFICIENCY OF INFORMATION SERVICES REAL-TIME ERROR CONDITIONS,
FAILURES AND DESTRUCTIVE INFLUENCES 320

Vaskova A.V., Mikhailichenko E.M.
TRANSPORT FACTOR AS A MEASURE OF ECONOMIC SECURITY 324

Verzun N., Kolbanev M.
SOME ASPECTS OF ENERGY EFFECTIVE COMMUNICATION 328

Kolbanev M., Mikadze S., Tatarnikova T.
PHYSICAL VOLUME OF BASIC INFORMATION PROCESSES 330

Korshunov I., Suvorova O.
THE ROLE AND PLACE OF INFORMATION TECHNOLOGIES IN THE FIELD
OF TRAINING 080101.65 "ECONOMIC SECURITY" 335

Levkina S., Mikadze S.
FOREIGN ECONOMIC EXPANSION: SIGNS OF THE CONDITION 338

Markelov K., Nechaev V.
BIOMETRIC TECHNOLOGY AS A FACTOR OF SOCIO-ECONOMIC SECURITY 342

Markov A. S., Fadin A. A., Tsirlov V. L., Rautkin Y. V.
CENTRALIZING OF INFORMATION SECURITY CONTROL 346

Moshak N.N.
INFORMATION SECURITY MONITORING SYSTEMS IN REGION OFFICIS OF BANK RUSSIA 348

Pichugin Yu. A., Kondrashkov A.V.
THE STATISTICAL ESTIMATION OF ECONOMIC STABILITY AND RISK ON THE BASIS
OF ALTMAN'S METHOD 352

Popova E.
MULTICRITERION OPTIMIZATION CHOICE OF INFORMATION SECURITY
SYSTEMS FOR COMPANIES 357

Erohin A. , Erohin V.
EFEECTIVE MULTI-ROBOT NAVIGATION METHOD, BASED ON A* PATH-FINDING ALGORITHM
MODIFICATION 361

Khanykov I.G.
TWO METHODS OF AUTOMATIC IMAGE SEGMENTATION COMPARISON..... 366

Ustinov I.
CHALLENGES, GOALS AND OBJECTIVES OF THE UNIFICATION OF KEY MANAGEMENT SYSTEMS CRITICAL INFRASTRUCTURE..... 371

Ustinov I., Igumnov V.
INFORMATION MANAGEMENT SYSTEM TO ENSURE INFORMATION SECURITY IN CRITICAL INFRASTRUCTURES 374

Gosudarev I.B.
E-LEARNING TECHNOLOGIES: SEMIOTIC APPROACH 377

Dmitrieva A., Klucharev A., Stepanov A.
REVIEW OF INFORMATION TECHNOLOGY USED IN EDUCATIONAL PROCESS DEPARTMENTS OF THE UNIVERSITY..... 380

Kolokolova L.P.
USING INFORMATION AND COMMUNICATION TECHNOLOGIES THE LESSONS OF THE RUSSIAN LANGUAGE 386

Laptev V., Noskova T., Flegontov A., Gavronskaya Y., Piotrowska X.
THE UNDERSTANDING OF CONVERGENCES OF HIGH-TECH SCIENCE AND NEW TYPE EDUCATIONAL ENVIRONMENT 389

Moglan D., Abramyan G.
EXPERIENCE OF USING OF EDUCATIONAL NETWORK COMMUNITIES BASED ON BLOGS IN TEACHING STUDENTS OF THE DISCIPLINE "INFORMATION TECHNOLOGIES" 394

Stepanov A., Kosmachev V., Shkirtil M. .....
INFORMATION TECHNOLOGY AS A MEANS OF STRUGGLE WITH PARALLEL THE EDUCATION MARKET 398

Stepanov A., Karaseva E., Zueva N., Moskaleva O.
COMPONENTS OF INFORMATION SECURITY TRAINING IN FUTURE ECONOMISTS 401

Stepanov A., Semenova E., Frolova E.
INFORMATION TECHNOLOGY TO IMPROVE THE QUALITY OF EVALUATIONQUALIFYING WORK STUDENTS 404

Tumaleva E.
VIRTUAL CONSTITUENT OF SCIENTIFICALLY-EDUCATIONAL ENVIRONMENT OF HIGHER SCHOOL INSTITUTIONS 4087

Abrahamian G.
RISKS AND POTENTIAL THREATS TO COMPUTER SYSTEMS AND E-LEARNING TECHNOLOGIES ON WINDOWS PLATFORM SCIENTIFIC AND EDUCATIONAL ENVIRONMENT OF THE RUSSIAN FEDERATION 414

Buinevich M. V., Bystrova O., Buchkova E.
PERSPECTIVE OF DEVELOPMENT AND RELEVANCE OF IMPLEMENTATION OF PROFESSIONAL STANDARDS 416

Solodyannikov A.V., Pilipov M.V., Fedorov D.Y.
REQUIREMENTS FOR ACCREDITATION OF COMPANIES INVOLVED IN THE INFORMATION SECURITY AUDIT..... 418

Bobonets S.A., Kuvatov V.I., Primakin A.I.
THE ISSUE OF APPLICATION OF STATISTICAL MODEL FOR EVALUATING TESTING OF KNOWLEDGE ON A SUBJECT MATTER CADETS TRAINING AREAS «INFORMATION SECURITY» IN THE EDUCATIONAL INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS RUSSIA..... 420

Zaleschansky B.D., Sviridov A., Pavlova O., Shalobina E.
SECURITY SYSTEMS ECONOMICAL SOCIO-TECHNICAL TRAINING OF PERSONNEL MANAGEMENT STRATEGY 425

Kuvatov V.I., Primakin A.I., Sineshchuk Y.I.
APPLICATION OF THE MODULAR PRINCIPLE AS FORMS OF THE ORGANIZATION OF EDUCATIONAL ACTIVITY WHEN TRAINING CADETS OF THE MINISTRY OF INTERNAL AFFAIRS ST. PETERSBURG UNIVERSITY OF RUSSIA IN THE SPECIALTY 090915.65 – «SAFETY OF INFORMATION TECHNOLOGIES IN THE LAW-ENFORCEMENT SPHERE» 429

Pooha G.P.
SYSTEMS OF INTELLECTUAL SUPPORT DECISION MAKING — INNOVATION DI-RECTION OF THE STUDIES AND PREPARATION IT-SPECIALISTS 432

Blank M.A., Blank O.A., Myasnikova E.M., Rudnitsky S.B., Denisova D.M.
DISTRIBUTION PATTERNS OF ANXIETY RATES IN ADULT HUMANS 438

Blum V. .....
EVENT MODEL DATABASE OF INTEGRATED EHR FOR SOLVING THE PROBLEMS OF MEDICAL STATISTICS 442

Blum V., Zabolotski V.
CLASSIFICATION OF SOFTWARE AGENTS FOR EARLY DEFECT DETECTION OF MEDICAL CARE BASED ON INTEGRATED HER 451

Inkin V.A., Delakova E.A.
THE DESIGN OF THE EXPERT DATA MINING DECISION SUPPORT SYSTEM FOR BIOMEDICAL RESEARCH ANALYSIS 460

Hodakov V.E., Sokolova N.A., Antypenko I.V., Babina O.V.
EVALUATION OF THE DEVELOPMENT OF CLASS COMPLEX SYSTEMS IN VIEW OF CLIMATIC FACTORS 464

Mihaiylov V., Perevaryukha A., Solovyeva I.
ANALYSIS OF PROBLEMS OF ICHTHYOCENOSIS OF THE MARINE ECOSYSTEM BASED ON COGNITIVE GRAPH MODEL 470

Perevaryukha A., Moseyko A.
PHENOMENOLOGICAL MODEL OF REPETITIVE OUTBREAKS OF POPULATIONS OF THE FOREST PESTS 475

Abrashkin A., Saushev A.
PROSPECTS OF DEVELOPMENT OF PROCESS OF SUDOPROPUSK BY INSTALLATION ON NAVIGABLE LOCKS OF THE AUTOMATED MANAGEMENT INFORMATION SYSTEMS 480

Alekseev A., Antipov V., Bobrovich V., Smolnikov A.
THE RANK OF PARTNER QUALITY CERTIFICATION: CONCEPT, THEORY, PRACTICE 485

Alekseev A., Tyurin I.
TECHNOLOGY MONITORING AND MANAGEMENT OF SECURITY INFORMATION RESOURCES OF INTEREST FOR MARINE ENGINEERING AND INFRASTRUCTURE 492

Alekseev S., Kirillovna E.A.
ALGORITHMS FOR DETERMINING THE COMPOSITION OF THE TECHNICAL MEANS IN NAVAL TRAINING SIMULATOR 497

Barkova N., Grishchenko D. .....
DIRECTIONS OF DEVELOPMENT OF INFORMATION-MEASURING METHODS FOR THE DIAGNOSIS OF ROTARY EQUIPMENT 503

Belousov I.V.
OPTIMUM SCHEDULING OF LOCKING SHIPS BY IDLENESS MINIMUM CRITERIA 508

Bobrovich V., Antipov V., Smolnikov A., Alekseev A., Musatenko R.
THE EXPERIENCE OF ORGANIZING THE RANK OF PARTNER QUALITY CERTIFICATION MARINE FACILITIES 511

Boriev Z.V., Sokolov S.S.
BIOMETRIC METHODS OF AUTHENTICATION: PRESENT AND FUTURE 517

Volkov V., Tichinin I., Alekseev A.
ANALYSIS OF THE SYSTEMIC ASPECTS OF MANAGEMENT DEVELOPMENT CRITICAL INTEREST IN MARINE ENGINEERING AND MARINE INFRASTRUCTURE 521

Grishchenko D.
INFORMATION-MEASURING SYSTEM OF RAPID DIAGNOSTICS ROTARY SHIPBOARD MACHINE 526

Yegorov A., Kuznetsov V., Nazargulov I.
PROGRAM SHELL OF PARALLELIZING FOR RESTORATION OF ACCESS TO DATA 530

Nekrasova A. A., Sokolov S. S.
SOME METHODS OF USING THE MODEL OF PERCOLATION PROCESS MODELING IN INFORMATION NETWORKS 534

Polenin V., Rebenok Y.
NETWORK PLANNING AND MANAGEMENT THE PERSPECTIVE DIRECTION OF PERFECTION OF THE AUTOMATED CONTROL SYSTEMS OF COURTS AND STRUGGLE FOR SURVIVABILITY 537

Polenin V., Mozhaev A., Mozhaeva I.
THE CONCEPT OF CONSTRUCTING A SYSTEM OF AUTOMATED SUPPORT MACRO-LEVEL ORGANIZATIONAL MANAGEMENT TASKS WITH APPLICATION OF NETWORK TECHNOLOGIES 540

Prikhodko V. M., Prikhodko I. V.
MATHEMATICAL MODELING OF DRYING CHARACTERISTICS OF SHIP ASYNCHRONOUS MOTORS 545

Kefeli I., Merkulov A.
THE MAJOR REASON OF THE COLLAPSE OF THE USSR 550

Azarov A., Abramov M., Tulupyev A., Tulupyeva T.
PROTOTYPE OF SOFTWARE FOR ANALYSIS OF PROTECTED OF USERS OF INFORMATION SYSTEM CONSTRUCTED ON THE BASIS OF ALGORITHM GRAPH TRAVERSAL SOCIAL TIES USERS 554

CONTENTS 566